European Commission

JRC TECHNICAL REPORTS

Enforcers and brand owners' empowerment in the fight against counterfeiting

Gianmarco Baldini (DG.JRC.E3)
Eduardo Cano Pons (DG.JRC.E3)

2017

Joint Research Centre

EUR 28400 EN

Contact information
Name: Gianmarco Baldini
Address: Via Enrico Fermi 2749, Ispra, Italy
Email: gianmarco.baldini@jrc.ec.europa.eu or gianmarco.baldini@ec.europa.eu
Tel.: +39 0332 78 6618

JRC Science Hub
https://ec.europa.eu/jrc

JRC104204

EUR 28400 EN

PDF	ISBN 978-92-79-64952-3	ISSN 1831-9424	doi:10.2760/135671
Print	ISBN 978-92-79-64953-0	ISSN 1018-5593	doi:10.2760/022485

How to cite: G. Baldini et al.; Enforcers and brand owners' empowerment in the fight against counterfeiting, 2017, doi:10.2760/135671

Title Enforcers and brand owners' empowerment in the fight against counterfeiting

Abstract
The objective of this report is to provide an analysis of techniques to empower law enforcers and brand owners in the fight against counterfeiting through the use of modern smartphones or similar devices. The report provides recommendations for standardization and deployment.

Table of Contents

Acknowledgements

The authors acknowledge and are grateful for the comments and recommendations made by DG GROW/J/2 (Jean Bergevin and Stephanie Martin), the European Union Intellectual Property Office (EUIPO) (Andrea Di Carlo, Massimo Antonelli, Valerio Papajorgji), UNICRI (Marco Musumeci), Reconnaissance International (Ian Lancaster), Brandstrike (Damian Broker), Indicam (Claudio Bergonzi, Sara Gabri), Philip Morris (Tamas Sipos Kacper Chmielewski), Alessandra Piloni (Italian Consumers Forum).

Executive Summary

This report was drafted by the European Commission – Joint Research Centre, Unit E.3 in close collaboration with the European Union Intellectual Property Office (EUIPO) agency and with its representatives Andrea Di Carlo, Massimo Antonelli and Valerio Papajorgji.

The objective of this report is to provide an analysis of techniques to empower law enforcers and brand owners in the fight against counterfeiting through the use of tools and devices that can help detect fake goods.

The report focuses on tools and devices that are easily available on the market, and divides them into two main categories. The first category is represented by modern smartphones (or similar devices, such as a tablet). The second category is represented by a wide range of portable devices that are different from smartphones (e.g. portable spectrometers). Most of these tools have already appeared on the market, although some of them may only be available in forensic labs (see [27],[29] and [30] for some examples of this category).

Although the analysis of techniques has been conducted from a wide perspective based on experts' opinions and updated literature, the authors' view favoured a combined approach, which is scientific and practical at the same time. Therefore, the report contains a practical description of the tools examined.

Each technique falling under the two categories is described in its application and use, and its features are compared in a grid built upon a number of metrics (e.g. requested resources, accuracy, adaptability to organisations and costs).

An overall evaluation showed that among the techniques that can be used with a smartphone, those based on barcodes and QR codes are the most cost-effective and have a good level of accuracy. Among tools of the second category (portable devices other than smartphones), the use of simple devices, such as polarised light, is the most suitable, particularly in terms of accuracy, adaptability to organisation, the level of training required and costs.

From the analysis, the concept of empowering was also an important element in supporting Due Diligence practices, and Supply Chain Integrity for manufacturers, which can authenticate goods in different parts of the supply chain and identify the presence of counterfeit products. Privacy aspects are also taken into consideration. Data collected by smartphones or portable equipment may disclose the user's personal information. Privacy risks and countermeasures in the specific area of the fight against counterfeiting are described.

Finally, the report suggests the following initiatives should be taken to foster better use of the technologies available within the EU.

1) Develop a common standard to empower the user for goods' authentication using the smartphone. In particular, the standard should define the generation of unique security identifiers (SIDs) and protocols between the smartphone and the remote reference library.

2) Create a specialised expert group within the European Observatory on Infringements of Intellectual Property Rights operating within the EUIPO to (a) monitor empowerment techniques appearing on the market; and (b) advise the EUIPO on integrating the most efficient techniques into its Enforcement Database (EDB), thus sharpening EU enforcers' capacity to fight against counterfeiting.

3) Create a standard query in the JRC's Technology Innovation Monitoring tool (TIM), specifically to enable the Observatory, and possibly its stakeholders, to monitor the evolution of anti-counterfeiting applicable technologies.

4) Implement an awareness knowledge management repository at European level, in collaboration with retailers and manufacturers, to be used and accessed by consumers through smartphones.

1 Scope and Definitions

1.1 Background and scope of the report

Counterfeiting is a longstanding problem that is growing in scope and magnitude. As described in the OECD (https://www.oecd.org/), counterfeiting is a concern to governments because of (i) the negative impact it can have on innovation (ii) the threat it poses to the welfare and health of consumers and (iii) the substantial resources channelled to criminal networks, organised crime and other groups that disrupt and corrupt society. The transborder dimension of counterfeiting as a crime has been analysed by Europol and the EUIPO in their '2015 Situation Report on counterfeiting in the EU' (https://euipo.europa.eu/ohimportal/en/web/observatory/observatory-publications), where it was reported that large-scale production of fakes implies well-organised networks of criminal groups, with a high awareness of enforcement tactics and the capacity to react accordingly.

The counterfeiting of goods is a concern to businesses because of the impact that it has on (i) sales and licensing, (ii) brand value and a firm's reputation, and (iii) the ability to benefit from the breakthroughs made in developing new products. IPRs' contribution to the economy and employment of the EU and, consequently, the damage caused by counterfeiting, has been widely examined by the EUIPO in its economic studies, targeting specific business sectors and geographical areas (see https://euipo.europa.eu/ohimportal/en/web/observatory/quantification-of-ipr-infringement).

Finally, counterfeiting is a concern for unaware consumers who are defrauded of the genuine product they have paid for and, with regard to specific types of goods, because of the significant health and safety risks that counterfeit (hence substandard) goods present.

Different techniques have been proposed to fight against counterfeiting. These techniques include identification and authentication technologies, processes to control supply chains and technologies to track and trace products.. A technique can be based on various tools and equipment. In this report, we will pay special attention to the use of the smartphone and other portable devices as tools to empower law enforcers and brand owners. We will analyse the techniques identified under a set of specific metrics to evaluate which are the most suitable.

The analysed techniques can also be an important element in supporting Due Diligence practices and Supply Chain Integrity, because the different categories of users can authenticate goods in different parts of the supply chain and report the presence of non-compliance (e.g. counterfeit products).

The structure of this report is the following: Chapter 2 describes the empowerment approach based on a smartphone. Chapter 3 describes empowerment by means of portable devices other than a smartphone. Chapter 4 identifies the main issues and challenges, including privacy aspects. Finally, Chapter 5 concludes this report and provides suggestions for possible next steps.

Disclaimer. In this report, specific case studies and anti-counterfeit products are mentioned to show the maturity of specific anti-counterfeiting technologies. It is not the intention of this report to endorse these anti-counterfeit products or the company producing them and they are only used as possible examples.

1.2 Definitions

This section provides the operating context and definitions of key terms used in this report.

Empowerment

For the aim of the report and considering the scope of the survey, the term empowerment indicates the act of enabling law enforcers (e.g. customs and police) and brand owners through techniques that can be used to distinguish counterfeit from genuine goods on the basis of available information, visual inspection and validation through tools 'readily' available.

The term 'readily' refers to techniques and tools that are widely available on the market and do not need sophisticated technological solutions and systems or complex training. In other words, the goal is to identify techniques that can distinguish counterfeit goods from valid ones without needing to use expensive forensic labs.

Users

While in literature and elsewhere, empowerment is associated with the concept of the 'consumer' in its widest sense (to encompass private citizens, enforcers and businesses purchasing products), in this report, law enforcement authorities, brand owners and enterprises — including small to medium-sized enterprises (SMEs) — are all considered as users.

More precisely, users include:

1) law enforcers, who want to check the validity of goods in the marketplace or in the customs area;

2) brand owners, who want to check the distribution of counterfeit goods impacting on their own brands in the marketplace;

3) enterprises, which cannot implement sophisticated or expensive controls for the goods provided by the supplier, such as forensic labs or responsible supply chain management;

4) retailers and distributors, who want to check that the received goods destined for sale or distribution are not counterfeit.

All these categories can use the empowerment techniques described in this report, with the following differences.

1) Law enforcers can have specific training to identify counterfeit goods and access portable equipment beyond a smartphone. Additionally, they can have access to knowledge databases to help fight against counterfeiting, such as the EUIPO's EDB, which provides a repository of product information and direct dialogue with brand owners, or other tools developed by other agencies (e.g. WCO, Europol, Interpol).

2) Whereas brand owners usually have specific knowledge of their own brand, they may have very limited or no knowledge of other brands.

3) Enterprises usually have specific knowledge of the range of goods used in their business (e.g. electronic components).

4) Retailers and distributors also have limited training, but they can be equipped with specific equipment if it is cost effective, advantageous for their activity or requested by law.

The differences in the users' approach will be considered in the assessment of techniques.

Techniques

The term 'techniques' is used to describe both technologies and approaches or a combination of both, which can be used in the fight against counterfeiting.

Since the purpose of this report is to analyse 'readily' available techniques (see above), two main categories of techniques based on different tools or equipment have been identified.

1. The first category is represented by the modern smartphone (or similar device, such as a tablet), which can be used as a tool to empower the user in the fight against counterfeiting. The modern smartphone is equipped with a high-resolution camera (e.g. 5 megapixels and above), support for different standards for wireless connectivity, a powerful processor able to support the implementation of sophisticated algorithms and support for Near Field Communication (NFC) and Radio Frequency Identification (RFID) readers. In addition, the smartphone can be integrated and augmented with a wide range of plug-in devices and tools (e.g. a USB microscope). This category will be the main focus of this report.

2. The second category is represented by the wider domain of portable products (e.g. portable spectrometers), which have already appeared on the market and can be used in the fight against counterfeiting in the field. In many cases, these portable products implement systems that have been available until only recently in forensic labs. An example of this is represented by the category of portable spectrometers. This report will also provide an overview of these systems, without specifying the product or the manufacturer.

In addition to the abovementioned tools, this category also includes low-cost tools, such as readily available chemical reagents or polarised filters.

Field

The focus of this report is on techniques to be used in the 'field', where field is the physical area where the user operates and where the goods are either exposed or in transit. In other words, it refers to physical locations, which are different from forensic labs, where goods that may need to be verified are placed, and that can coincide with:

- the enterprise's premises
- the marketplace
- the customs area.

Consequently, we will not explore empowerment techniques for e-commerce as the user does not have physical access to the goods.

1.3 Metrics

The following metrics will be used to evaluate the techniques described in this report. An evaluation analysis of the techniques is presented in the subsequent chapters of this report.

1. Requested resources

This metric is used to determine how many resources are required to deploy and operate each empowerment technique. Resources can include technological devices (e.g. a smartphone), electric power, people and communications.

2. Accuracy in detecting a fake

This metric is used to evaluate the accuracy of the technology to detect a counterfeit product. For example, to what extent are spectroscopy scanners accurate enough to detect counterfeit textiles? Note that accuracy could be affected by the risk of cloning. If the authentication information can be easily cloned, the score for accuracy will be low.

3. Need for adaptation to organisations and existing processes

This metric is used to evaluate the impact on organisations and already existing processes for law enforcers and brand owners/SMEs. For example, if the adoption of the new technology requires the implementation of new complex processes, this could be a negative factor.

4. Requested level of training

This metric is used to evaluate the level of training required to operate the techniques. It is measured as a positive metric. A higher value equates to a lower level of training.

5. Robustness and adaptability to environmental conditions

This metric is used to evaluate whether environmental conditions can have a positive or negative impact on the use of the technique. For example, darkness can have a negative impact for empowerment techniques based on image processing; this is not an issue, however, for techniques based on radio frequency authentication.

6. Flexibility to support multiple applications

This metric is used to evaluate whether the proposed technique and related tools can be used to perform multiple authentication solutions and processes. For example, an application against counterfeiting, which targets only specific brands, is of limited use for law enforcers, who will be forced to use many different applications.

7. Upgrade capability

This metric is used to evaluate the future extendibility of the technique. It evaluates how tools and processes used for the technique can be extended in the future.

8. Cost

This metric is used to evaluate the cost for the users to deploy and operate the technique. We separate any costs afforded by consumers from those borne by owners/manufacturers.

9. Market and standardisation support

This metric is used to evaluate the market and standardisation support by the stakeholders. If a technique is not widely deployed in the market, this could be an issue for law enforcers because they could be locked in to a specific technology or tool. This metric also includes the maturity of technical support or the repair of tools used in the empowerment technique.

10. Interoperability with existing open tools

Whether and how technology can be adapted in order to be incorporated into existing technological tools and cost-free for both law enforcement authorities and IPR holders, such as the EUIPO's EDB, or others.

2 Empowerment via Use of a Smartphone

2.1 Capabilities of a smartphone

A description of the approach to empowerment via use of a smartphone is presented in Figure *1*.

Figure 1. Empowering the user in the fight against the counterfeiting of goods with a smartphone

The centre of the suggested approach would be a smartphone, that is to say, a tool used nowadays by all relevant users. The smartphone acts as a field sensor (to detect optical features, read RFID tags, geolocations etc.), telecommunication gateway (to obtain real-time information on the object or to allow direct interactions between the object and a remote verification system) and notification system (to provide information to the track and trace supply chain system).

Furthermore, the smartphone can be connected to other systems and components, such as the producer's supply chain, the law enforcer's reference database and other systems.

More precisely, nowadays a smartphone (June 2016) has the following capabilities:

1) A high-resolution camera. It is now commonplace to buy a smartphone with a 5 megapixel (MP) camera for under EUR 100 and the trend will continue, so we can envisage that new cameras will have an even higher resolution.

2) Wireless connectivity through different wireless communication standards: Wi-Fi, GSM, Universal Mobile Telecommunications System (UMTS), Long Term Evolution (LTE) and with broadband capacity. This ensures that data can be sent quickly to a remote server (e.g. cloud database) or a remote application.

3) High-performance computing platform. Today's smartphones have similar computational power and capabilities to the older desktop computers, and this trend is likely to continue.

4) Near field communication (NFC) readers to read high-frequency (HF) RFIDs, which both operate at the 13.56 MHz frequency.

5) Global Navigation Satellite Systems (GNSS), which can record the time and space when goods are being evaluated.

6) Plug-ins of different components through the USB interface. For example, visual augmentation equipment (e.g. USB microscope) or a DVB dongle (e.g. to collect radio frequency emissions) can be added to a smartphone.

7) Installation and activation of applications on a smartphone, which can implement anti-counterfeiting applications.

Most of these capabilities were not present in smartphones until recently, so it was relatively difficult to implement anti-counterfeiting techniques. The new capabilities mean that it is possible to implement various techniques, which will be described here. This possibility has also been reported recently in the media, see [8],[9] and [10].

In the context of the fight against counterfeiting, the smartphone itself is the component (in the hand of the law enforcement official or the representative of a brand owner, namely the 'users') of a wider system, which can include an application, a communication protocol, a reference library, a brand owner database of the product features, or a database linked to the supply chain and other elements. The smartphone is used to collect data (e.g. images, RFIDs) from the goods to be evaluated. This data can be processed in the smartphone itself (e.g. to extract features) to generate additional information from the raw data using an application. The application sends the data and the information to a remote application using wireless connectivity and a specific communication/data protocol. Additional information can also be sent from the smartphone, such as its position if the privacy settings defined by the user allow this (see paragraph 4.1). The remote application uses a reference library or a supply chain database to match the data and information received from the smartphone. The matching information (i.e. the product is counterfeit) and related data (e.g. for which market the product is produced) is then sent back to the smartphone. Then, the application in the smartphone displays this information and data to the user. This generic workflow is represented in the following figure:

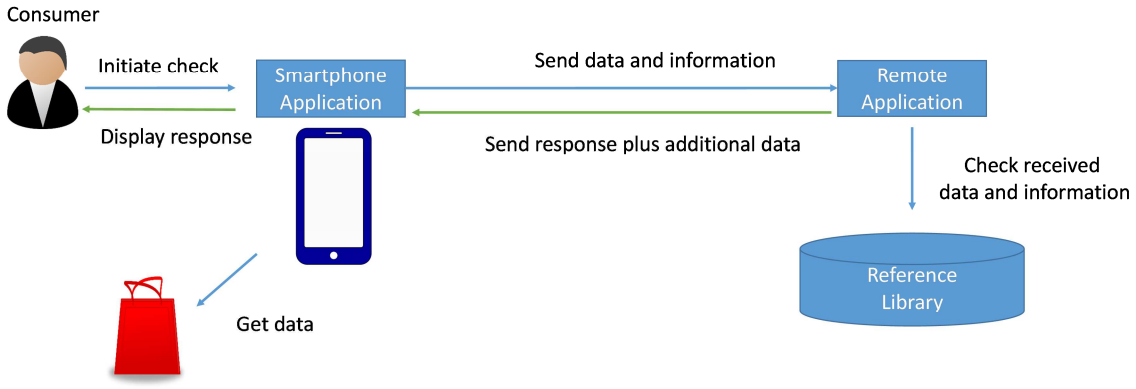

Figure 2. Generic workflow

The users only see and use the smartphone, but adequate infrastructure must be built to implement the anti-counterfeiting technique. This is described in the following paragraph.

2.2 Main components of a smartphone-based approach in the fight against the counterfeiting of goods

Beyond the smartphone, a complete solution must include the following elements.

1) **Smartphone application**. This is the application running on a smartphone, which implements a Graphical User Interface (GUI) to the user to receive requests. The smartphone is connected to the main sensors of the smartphone to collect the required data (e.g. images). The application can also implement specific algorithms to process the data. For example, it could extract statistical features from the retrieved image. The smartphone application is also responsible for sending the data and any additional information (e.g. features, position or privacy settings) to the remote application using a well-defined communication protocol.

2) **Communication protocol**. This communication protocol is responsible for sending the data and information from the smartphone application to the remote application and sending back the response from the remote application to the smartphone application.

3) **Remote application**. This is the remote application hosted on a remote server, which also uses the communication protocol to exchange data with the smartphone application. The remote application uses the information from a reference library to evaluate whether the received data and information from the smartphone identify counterfeit goods.

4) **Reference library**. This is the database of the matching information (e.g. track and trace or fingerprinting for product identifications), which can be created by brand owners or by other organisations that collect the information that identifies valid goods from several brand owners. The reference library is a generic term, which can include many different types of information, for example, the fingerprinting of goods or the serialisation number of an overt/covert tag. Note that the reference library can also be used to insert additional information useful for the different categories of users. In Europe, a potential implementation of the reference library could be through the EDB, managed by the EUIPO [1]. In fact, the EDB could be ideally suited to building a reference library gradually with contributions from various brand owners. For example, the tax regime of a specific market can be inserted in the record of the reference library for specific goods. In this way, the user (e.g. law enforcer) can detect goods, which should not be present in the area where it has been evaluated. This capability is very important to counter the threat of smuggling.

2.3 Specific empowerment techniques

We can distinguish different empowerment techniques based on smartphone information, how the reference library is created and what type of information is stored or collected by the smartphone.

1) **Reference library created by the brand owner during the manufacturing process**. The reference library is created by the brand owner itself or by a company working for it and the specific information on the single product is collected and stored in the reference library during the manufacturing phase. In other words, the manufacturing plan of the brand owner is equipped with systems and devices to collect the unique

[1] Enforcement Database: https://euipo.europa.eu/ohimportal/en/web/observatory/enforcement-database.

fingerprinting of the product and/or the package, which is then stored for future use. Note that the fingerprinting information can be in different forms: it can be a serial number represented in the barcode or QR code, it can be a fingerprinting of the product itself on the basis of its physical or chemical properties, or it can be the RFID applied to the product and/or the package. It can also be a serial number embedded in an overt or covert tag. In fact, a combination of these fingerprinting methods can also be used to improve authentication accuracy and resistance to the threat of cloning. In this case, the reference library must store the correlation of the set of data used to identify the package and/or the product uniquely.

2) **Reference library created by a commercial third party, which works with the brand owner**. In this case, the reference library is created by a third party, which works with the brand owner to insert its own tags. The tag is applied to the product after the manufacturing process. As a consequence, it is not an intrinsic property of the product. The difference with the previous case is that a correlation between the tag identifier and the product must be done before the product is distributed on the market. This can increase the risk of cloning or removal of the tag. The advantage is that the brand owner does not need to invest in anti-counterfeiting technology if it lacks skills, competences or economic capabilities (e.g. because it is a small company with a limited budget), as the commercial third party will perform this activity.

3) **Reference library created by another third party**. In this case, the reference library is created by another party different from the brand owner, even if it may collaborate with the brand owner. For example, the third party can be a public body that collects information from different brand owners, with the aim of helping competent authorities detect counterfeit goods on the basis of specific features: images of badly formed logos, use of the same identification number in the barcode, QR code or RFID etc.

A good example of such a library is provided by the EUIPO's EDB, a cost-free knowledge-based system fed by brand owners, law enforcement authorities and the EUIPO, containing a wide range of information to support the protection of IPRs. Through appropriate technical solutions, the EDB might work as a reference library and provide a wide range of information to different categories of users, such as:

- product identification
- product images
- packaging
- supply chain
- IPRs
- details of past infringements.

Law enforcement authorities in particular might have direct access to information when they have suspicious products in front of them in the course of their front-line activities in customs areas and the marketplace. Through scanning or reading codes or other technologies placed on the product or its packaging, an application may submit the results stored in the EDB.

In principle, this functionality might also be extended to external users of the EDB, such as enterprises acting in the supply chain that need to verify the authenticity and details of goods they are dealing with, as well as to private consumers at a point of sale.

Through appropriate technical solutions based on interoperability between databases, the EDB might be connected to other similar repositories available on the market (e.g.

GS1 database for barcodes, WCO-IPM); it might also host reference libraries created by brand owners, in order to integrate the reference library accessible to users.

2.3.1 Reference library created by a brand owner during the manufacturing process

In this case, the brand owner collects the data to identify the goods in the supply chain or manufacturing process itself. The data can be defined and extracted using different authentication technologies. For example, it can be the specific signature of the paper of a packet of cigarettes (taken with an image) or it can be the identifier of an RFID embedded in the fabric of a luxury bag.

The choice of the serialisation and authentication technology is really dependent on many factors: the type of goods, the impact of the authentication technology in the manufacturing process, the associated costs and so on. For many consumer goods, barcodes, QR codes or simple overt/covert technologies can be used, while more sophisticated and expensive goods can use RFID or more complex authentication technologies.

The goal is to collect and store identification and authentication information, which can be correlated with the data extracted by a smartphone in the field. This means that the data generation and collection process in the manufacturing plant must be designed together with the definition of the application in the smartphone or the related protocol.

A pictorial description of the process is provided in Figure 3.

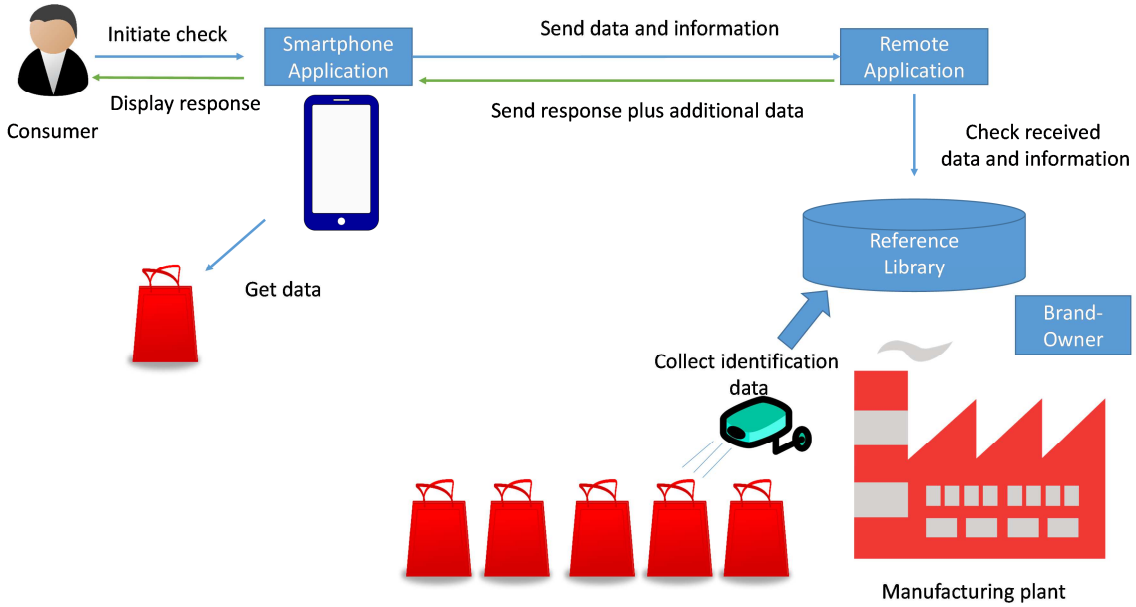

Figure 3. Brand owner based technique

Supply chain information, such as the tracking and tracing of data, can also be used for this purpose if the brand owner so desires. In this case, we must distinguish between closed-loop track and trace supply chains.

- A **closed-loop** supply chain is when the manufacturer, retailer and distributor are the same entity and the tracked goods are controlled by the same business entity (either directly or indirectly).

- An **open-loop** supply chain, meanwhile, is where the tracked goods can be distributed to different business entities, each of them equipped with its own back end. This difference is quite relevant to supporting the empowerment concept because in closed-loop, the ICT infrastructure is not designed to share information on the tracked goods with external entities. In open-loop, the extension to the end user is relatively straightforward and the associated costs are similar to the implementation of an Android application and connected to a remote back-end infrastructure (e.g. a cloud infrastructure).

Another aspect to be considered for the development of an empowerment solution is related to information sharing among the different back-end systems, which store the tracking information on the goods. The back-end systems should be capable of exchanging information with similar data formats. In addition, security and access control solutions should be developed to protect sensitive data, but also to guarantee access to the end users or the empowerment back-end systems, which are responsible for matching the information collected by end users. All these factors contribute to the overall cost of the empowerment solution.

The authentication information can be collected not only on the goods itself but also on the packages, which store the goods in a recursive way. In other words, the packages containing the goods can be authenticated as well. Recursive means that this process can be repeated for the larger packages storing the smaller packages. In this way, the user can trace the goods better, which can also be used to identify gaps in the tracing chain and pinpoint the presence of counterfeit goods.

A good example of this technique is CODENTIFY [11], developed by the Digital Coding & Tracking Association, which represents some of the world's largest manufacturers of tobacco products. As described in [11], CODENTIFY can support:

- tracking and tracing — enabling the electronic monitoring of products as they move through the supply chain and the tracing backwards of their journey history to identify potential points of diversion;

- product authentication — enabling anyone, anytime, anywhere to immediately verify the authenticity of a product using widely available technologies, such as a mobile phone or the internet;

- digital tax verification — enabling governments to verify and control online the volume of products manufactured and so calculate the commensurate amount of excise and other taxes due.

An analysis of the use of CODENTIFY in the tobacco industry is also given in [39]. Currently, CODENTIFY is only used in the tobacco industry and it should be studied to see whether it could also be used in other sectors.

In the pharmaceutical sector, a similar serialisation and tracking system is going to be set up under Commission Delegated Regulation (EU) 2016/161 of 2 October 2015, which was published, after scrutiny by the European Parliament and the Council, on 9 February 2016. The Delegated Regulation, and the new medicine verification system it lays down, will apply as of 9 February 2019.

This new system is based on a unique identifier, defined as a 2-D Data-Matrix code, developed to ISO standards (GS1).

The key data elements are:

- product code (14-digit)
- randomised unique serial number
- expiry date
- batch number
- (national reimbursement number or other national number (where necessary)).

The serialisation is based on a random number. The validity check (i.e. verification) of the serial number will be done at the point of dispensing (e.g. the pharmacist) by using a central cloud system, which stores and updates the status of the tracked pharmaceutical products. The cloud system will be called EMVO — European Medicine Verification Organisation, responsible for the operation of the European hub.

A Swedish pilot project (designed and deployed in 2009/2010) was implemented successfully to high levels of satisfaction from the stakeholders involved (e.g. pharmacists and wholesalers).

A German pilot project securPharm (http://www.securpharm.de/en/index.html) was implemented successfully. Coding is written in the Data Matrix code in accordance with ISO/IEC 16022. After an operating time of more than three years, the securPharm project is well on its way. The stakeholder associations have started a system for the verification of pharmaceuticals that meets the requirements of the EU Falsified Medicines Directive and works under real-life conditions. Further details on the securPharm project and its status are in [38].

Another example where the intrinsic features of a product taken during the manufacturing process are used to empower the user is described in [10]. The electronics maker NEC has developed an authentication system that compares images taken with a smartphone with those in a cloud-based database. Images of the authentic product from the manufacturer would need to be registered beforehand. As described in the report, this can be applied to the retail sector or any other product, which can be identified through augmented visual inspection. NEC stated in [10] that the technology is currently in the testing phase and the firm plans to release a commercial version in 2015, but at the time of drafting this report (January 2017), no commercial versions are still available.

The know-how makes use of fine patterns in the grain of metal or plastic that occur naturally during manufacturing and are invisible to the human eye.

The system can be used to find pirated goods, to trace the origin and distribution through the marketplace of authentic goods and to manage components in industrial applications such as maintenance and repair work, making sure they are being used correctly.

2.3.2 Reference library created by a third party working with a brand owner

In this case, a commercial third party that has developed a technology for authentication or track and trace, works together with the brand owner to apply identifier tags to the goods during the manufacturing process or after the manufacturing process and prior to distribution. This case is different from the previous one, because the authentication information (e.g. overt tag) is not an intrinsic part of the product but it is applied to it. Note that the identifier tag could be part of the supply chain integrity process and similar

considerations of the open and closed supply chain described in paragraph 2.3.1 **Reference library created by a brand owner during the manufacturing process** also apply to this case.

The overall workflow is described in Figure 4 below. The commercial third party applies its own identification and authentication tags to the goods after they are produced at the manufacturing plant and before distribution to the market. The identification and authentication data is then stored in the reference library. Usually, the commercial third party has also developed a remote application and smartphone application to implement the overall workflow.

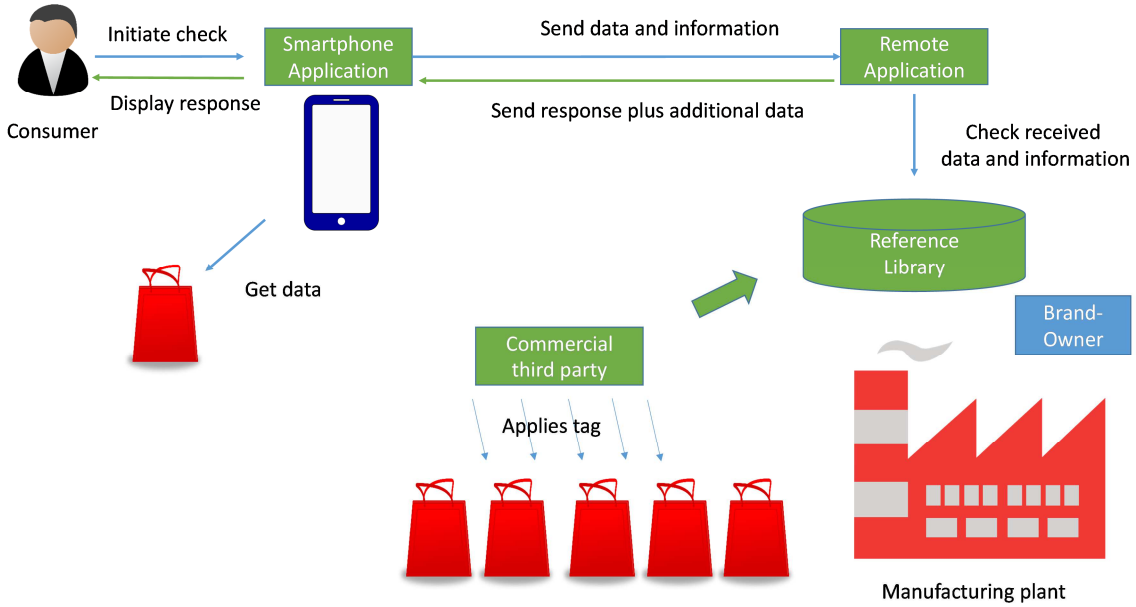

Figure 4. Technique based on brand owner and third party

This technique is more appropriate for small companies that cannot afford the implementation of a technique such as the one described in paragraph 2.3.1 **Reference library created by a brand owner during the manufacturing process** and for the types of product where a tag cannot be inserted during the manufacturing process.

Another advantage of this technique is that the commercial third party, which has developed the technology, can create a single smartphone application, a single communication protocol and a single reference library for different categories of goods and brands, thus facilitating the checks by the user.

These techniques have been developed by various companies around the world. One example is SICPATRACE from SICPA [12]. In a first phase, called secure marking, the SICPA Data Management System generates a unique reference code for each ‘unit’. This unique reference code can be applied to the goods during the manufacturing process. The reference codes can include overt, semi-covert and covert features.

Subsequently, each code is activated by SICPA on the production line, thus enabling online oversight. In the third stage — distribution control — the codes are scanned as the products move along the supply chain. Each scan sends data to the Data Management System (the equivalent of a reference library), which aggregates the details of the product’s path until the final point of sale.

Users are able to identify and trace products with the SICPAMOBILE® handheld inspection device, which securely authenticates and reads the unique codes.

Another example of this system is Authenticateit (see [13]), which is a smartphone application that empowers users with a fast and convenient way to check an item's authenticity before purchase, while offering brand owners a powerful tool to track, trace and prevent instances of unauthorised distribution and retailing. Authenticateit works with the industry-standard GS1 barcode.

2.3.3 Reference library created by a third party other than brand owners

In this technique, the reference library is created by a third party on the basis of reported information on counterfeit items. For example, a consumer association or law enforcement agency can build a knowledge-based system, which includes a reference library to indicate the most common cases of counterfeit items. A user can check the validity of goods by sending relevant authentication data to a remote application linked to a reference library. The response from the remote application will give a probability to the user that the identity of the product is what it claims to be. In a similar approach, the remote application can provide data or digital information (e.g. images) to help the user identify the goods.

An alternative way is that the brand owners provide information to build the reference library or notify the potential presence of a counterfeit item. One example of this technique is uFaker (see [14]), where a user can take a picture of a possible counterfeit item and send this information together with the location to a remote cloud application, which notifies the brand owners.

A description of how the EUIPO's EDB may serve the purposes of a unique reference library has been given in paragraph 2.3.

An example of the data flow in this technique is shown below:

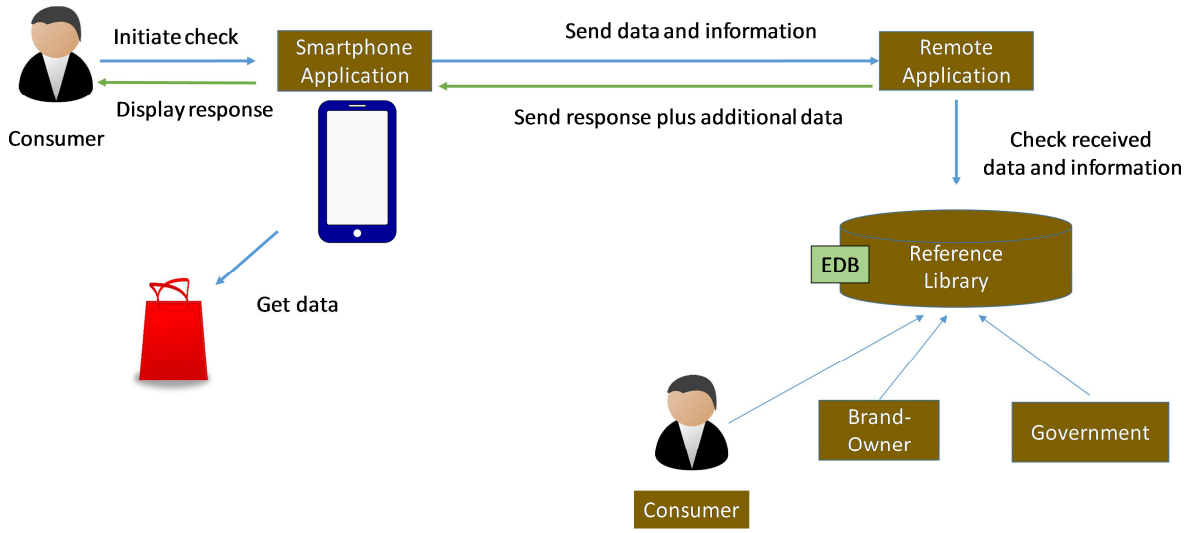

Figure 5. Reference library created by third party other than brand owners

The advantage of the EUIPO's EDB is that, as a reference library, it can include many different types of goods from different brands and it can process and receive input from many different categories of stakeholders, which can examine counterfeit items in different ways.

Another important advantage of implementing the reference library through a public body is that it becomes a central point of contact across Europe and for different private organisations. In this way, the standardisation of the reference library formats and input data processes is easier to achieve.

The main disadvantage of this type of option is that the information stored in the reference library may be inaccurate, incomplete or not up to date. For example, new types of counterfeit goods may not be included in the reference library in time for a proper evaluation. To address this potential issue, it is important to build strong relationships with brand owners in the first phases of the implementation of the reference library. From this point of view, organisations such as the EUIPO, which already has a network of contacts at European level, could be ideally suited to address this issue.

2.4 Costs analysis

The costs associated with the design and deployment of anti-counterfeiting solutions to empower the smartphone user are structured in the following way:

1) **Design and implementation of the mobile application**. This is the cost of developing a mobile application that can be installed on a smartphone and supports solutions that empower enforcers and other relevant users in the fight against counterfeiting. The application must be designed to interact with the smartphone's sensors, which are needed to collect the requested data, such as images, NFC readings, track and trace information and GNSS position.

2) **Reference library**. This is the cost of developing the reference library, which is used to compare the identification data collected in the field with the database of identification data stored before the goods are distributed on the market. These costs can also be based on different elements: a) the implementation of the means to collect data in the manufacturing or distribution processes, b) the creation of a database to store the reference data, c) the development of the remote application to make available and manage the reference library and d) the publication of the reference library on the web to be accessible by the mobile application. Other associated costs, such as the development of standards or protocols, are described in the other items of this numbered list.

3) **Development of standards**. This is the cost of developing standards for: a) the definition of the protocol between the smartphone and the reference library, b) the format of the data stored in the reference library, c) the serialisation coding to identify the goods in the reference library, d) the back-end systems used to support the supply chain. These should be interoperable and use a similar data format (e.g. based on an OASIS standard).

4) **Open-loop v closed-loop supply chain**. If the empowerment solution has to be built on a closed-loop chain, extensive and costly modifications to the supply chain will be required. This is not the case for an open-loop chain, which is designed to support different entities. As a consequence, one relevant cost can be associated with the integration of the ICT systems used to support the supply chain with the reference library. Note that the integration between the two systems does not need to be complete. In other words, not all supply chain data can be used in the reference library, as some of it can be proprietary to the brand owner.

5) **Privacy, security and access control**. This item includes various elements, which address the privacy and security aspects of the empowerment concept. Privacy

aspects can be quite important for users. If they are not addressed, the deployment of applications to empower the user in the fight against counterfeiting can be hampered because average citizens can fear that their personal data is at risk when sending data about the goods. In addition, different categories of user (e.g. law enforcers, brand owners) can have different access to the reference library data. For example, law enforcers can also use data based on covert features rather than on overt features. In addition, access control functions may be required to ensure that only the reference library can be accessed by the web and not other data systems, which store sensitive information.

2.5 Authentication technologies

This section briefly describes authentication technologies, which can be used to identify and authenticate the goods in the field against a reference library.

Note that a detailed description of all the potential authentication technologies for fight against counterfeiting is not in the scope of this report. A previous report drafted by the JRC (JRC98181) has described extensively the various technologies including the ones used in forensics labs.

In this section, the focus is only on authentication technologies, which can be supported by the capabilities of the smartphone.

2.5.1 Numeric Identifier/One-dimensional barcode

This was the first technique used to serialise products and, with this information, to track and trace goods in a supply or distribution chain. The first implementation was the Universal Product Code (UPC), which has been a dominant barcode standard in North America since it was established in the 1970s.

The UPC has evolved into various versions, for example, UPC-A and UPC-E.

At international level, the Global Trade Item Number (GTIN) is an identification number that may be encoded in UPC-A, UPC-E, EAN-8 and EAN-13 barcodes, as well as other barcodes in the GS1 system.

Numeric identifiers based on barcodes have been used extensively for many years around the world, and they remain the most used track and trace or identification technique.

As extensive literature is available on this technique, we refer the reader to related references. For example, for GTIN see [15].

There are various examples of the smartphone's ability to read and analyse barcodes, therefore this can be considered a very mature technology.

2.5.2 QR codes and other two-dimensional barcodes

The QR (Quick Response) code is a two-dimensional (2-D) barcode.

In comparison to one-dimensional barcodes, the QR code is able to store more information in the same space. QR codes are designed to be read and understood (decoded) by

computers, using machine-vision systems consisting of optical laser scanners or cameras and barcode-interpreting software.

Unlike 1-D barcodes, the QR code is a 2-D matrix code that conveys information not by the size and position of bars and spaces in a single (horizontal) dimension, but by the arrangement of its light and dark elements, called ‘modules’.

The QR code has a number of advantages in comparison to a one-dimensional barcode. The main advantage is the high-capacity data storage, as a QR code can store hundreds of times more data than a one-dimensional barcode. The QR code is also more robust against curved surfaces or errors due to marks or spots.

There are various examples for the use of the smartphone to read and analyse QR codes, therefore this can be considered a very mature technology.

2.5.3 Physical fingerprint technology on visible spectrum

Physical fingerprints use the specific characteristics of the base material or the packaging. For instance, paper, cardboard, metal and plastic are made up of tiny fibers in random orientations, which are naturally unique in their structure. According to this, every package has its own microscopic structure, its own fingerprint, which cannot be rebuilt and cannot be removed. For authentication to be secure, it is important to use this technology directly on the base material of the smallest packaging available to users; fingerprints of labels, stickers or banderoles will verify the attached strip but not the packaging onto which these are applied.

In this context, we include any physical fingerprint technology regardless of the medium (i.e. material) where it is applied: holograms, paper, inks, security threads and regardless of whether it is overt or covert.

For greater security, it is possible to combine a printed unique identifier as the visible element and a physical fingerprint of a package as the invisible element of a security feature. On a mass production line, each package can be scanned and its unique fingerprint can be recorded and linked to its specific unique identifier. When checking, regardless of whether a package is genuine or not, the system compares the physical fingerprint on the base material to the digital fingerprint embedded in (or retrieved from) the unique identifier.

The use of the smartphone to read and analyse physical fingerprint technology is a recent development, but it is supported by an increasing number of companies thanks to the smartphone’s higher-resolution camera.

Various companies produce these products, some of which are listed below. The intention is not to recommend these products specifically, but to show the maturity of this technology:

- VERIFYME (see [17]), where the integration of physical security pigment technologies with digital verification solutions creates an anti-counterfeiting system by which anyone with a smartphone can authenticate material goods. The patented technology uses smartphones in two ways. The phone’s internal ‘flashlight’ changes the colour of the visible ink identification mark on the package. In addition, the technology leverages the device’s camera to detect and recognise a QR code, or similar embedded invisible mark. By communicating with the brand via a special application, the user is assured that the product is genuine, not fake or a cheap, potentially dangerous, knock-off (from [17]).

- Arjo (2015) (see [18]). This company has developed a technology called Signoptic™, which is a patented technology based on a vision system converting the texture of a product into a unique signature thanks to a proprietary algorithm. Because the signature is generated from non-duplicable aspects of the product itself, Signoptic™ allows both identification and authentication. Signoptic™ can be used directly on the product (primary packaging), at the packaging level (secondary packaging) or directly on labels.

- ProofTag (see [19]) has developed various solutions including Ramdot™, which is a security feature based on the dispersion of optical variable particles. In Ramdot™, particles are scattered in a random manner, thus creating a unique distribution of optically variable elements. Ramdot™ technology can be applied to several components, such as security seals, shrink sleeves and textile tags. The product can be customised in terms of the particles' colours, tactile aspect, and their visible metallised effect. The visual matching of the pattern versus its recorded image allows for easy identification of the marked object.

Note that these solutions can be both overt or covert and they can be applied both by the brand owner in the manufacturing process (as described in paragraph 2.3.1 **Reference library created by a brand owner during the manufacturing process**) or applied to goods in the distribution phase using a tag (as described in paragraph 2.3.2 **Reference library created by a third party working with a brand owner**).

2.5.4 Radio Frequency Identifier (RFID)

An RFID tag is basically a device composed of a small chip connected to a coil. The chip is essentially a state machine with a memory, providing limited storage and computational capabilities. To communicate with such devices, an RFID tag reader has to be used. The reader emits a radio frequency (RF) field that by induction through the coil powers the chip. At the same time, the reader itself modulates the field to code commands sent to the chip, which in turn replies to the reader modulating the same field, so establishing a bi-directional communication.

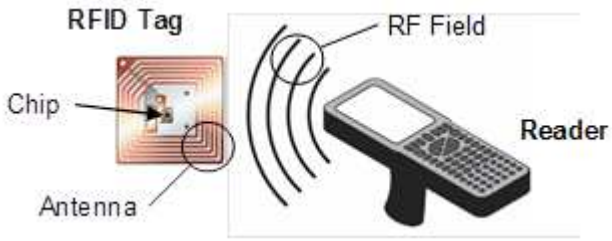

Figure 6. Radio Frequency ID

The main purpose of an RFID tag is to memorise data and release it when queried by a reader; usually, at least a unique identifier (ID) is stored in the chip. According to this peculiarity, one of their main applications is item labelling.

RFID tags can be stuck onto or embedded in items to track their position, reading the tags at different places, and to receive information about them easily, storing specific item-data in each applied tag. The information gathered from a tag can also be related to additional item data stored in a back-end system.

A smartphone with an NFC reader can read some types of RFIDs but not all of them, even if various RFID readers connected to USBs are available on the market. Passive RFID tags primarily operate at three frequency ranges:

- low frequency (LF) 125-134 kHz
- high frequency (HF)13.56 MHz
- ultra high frequency (UHF) 856 MHz to 960 MHz.

Near-field communication devices operate at the same frequency (13.56 MHz) as HF RFID readers and tags. The standards and protocols of the NFC format are based on RFID standards outlined in ISO/IEC 14443, and the basis for parts of ISO/IEC 18092.

The RFID can be inserted in the product if the type of product and its material composition allows. For example, an RFID can be inserted in the fabric of a luxury bag, but it is more difficult to insert an RFID in a semi-conductor chip. In other words, RFID technology can be used both by the brand owner in the manufacturing process (as described in paragraph 2.3.1 **Reference library created by a brand owner during the manufacturing process**) or applied to the product in the distribution phase using a tag (as described in paragraph 2.3.2 **Reference library created by a third party working with a brand owner**).

2.5.5 Collection and analysis of images of the object to be authenticated

In this solution, the user collects an image of the object to be authenticated and uses algorithms to provide an estimate that the image is related to a valid (non-counterfeit) product.

An example of this solution has been announced recently by NEC in [10]. The electronics maker NEC has developed an authentication system that compares images taken with a smartphone to those in a cloud-based database. Images of the authentic product from the manufacturer would need to be registered beforehand. As described in the report, this can be applied to the retail sector or any other product that can be identified through augmented visual inspection.

NEC reported that the technology is currently in the testing phase and the firm plans to release a commercial version in 2015, but at the time of writing this report (January 2017); there is no report on the availability of such products on the market.

The article points out that ‘object fingerprint authentication technology’ is the first such system in the world that can identify individual objects, according to the company.

The know-how makes use of fine patterns in the grain of metal or plastic, which occur naturally during manufacturing and are invisible to the human eye.

This technique is slightly different from the technique described in paragraph 2.5.3 **Physical fingerprint technology on visible spectrum**, because the image captures fingerprints, which have not been inserted deliberately, but which are created spontaneously during the manufacturing process. From this point of view, this technology does not require changes to the manufacturing process of the material but it may have less accuracy than the technique described in paragraph 2.5.3 **Physical fingerprint technology on visible spectrum**.

The system can be used to find counterfeit goods, to trace the origin and distribution through the marketplace of authentic goods and to manage components in industrial applications, such as maintenance and repair work, ensuring they are being used correctly.

This is an example of the technical and commercial feasibility of the empowerment application, at least based on images.

An additional issue about this solution is that techniques of pattern matching based on the images of dress and apparel can lead to false alarms due to damage to the product's fabric or different light conditions, etc. There is extensive literature available on the pattern matching of images, which identifies the main challenges for accurate identification (see, for example, [20]).

2.5.6 Analysis of the different techniques

The evolution of the technology has paved the way for the use of the smartphone to identify and authenticate goods and to distinguish them from counterfeit goods.

In this section, we compare the different techniques to highlight the related advantages and disadvantages.

The techniques based on the unique fingerprinting of goods, as described in paragraphs 2.5.3 **Physical fingerprint technology on visible spectrum** and 2.5.5 **Collection and analysis of images of the object to be authenticated**, are more accurate and robust against cloning attacks because it is quite difficult for counterfeiters to reproduce exactly the unique fingerprint of goods. However, it may not be possible to obtain fingerprints of all the different materials using the smartphone features. Note that in this section we are only focused on fingerprints, which can be validated with the basic features of a smartphone. The use of portable devices is described in another section.

Even with these limitations, there is now a large variety of products on the market where physical fingerprints can be inserted into common materials used for packaging, such as paper or special plastics.

The technique described in paragraph 2.5.3 **Physical fingerprint technology on visible spectrum**, where artificial fingerprints are inserted into the product or when a specific material is used to increase the uniqueness of the product, is more efficient than the technique described in paragraph 2.5.5 **Collection and analysis of images of the object to be authenticated**, for obvious reasons: in the former technique, the material is designed to collect unique fingerprints, while in the second technique, the uniqueness or the preservation of such uniqueness against a change in the environment is not guaranteed. Note that the technique described in paragraph 2.5.3 **Physical fingerprint technology on visible spectrum** can also be used in tags applied to the product or to packaging containing the product.

The technique described in paragraph 2.5.5 **Collection and analysis of images of the object to be authenticated** does not require the application of special solutions in the manufacturing process.

The advantage of the barcode or QR code described in paragraphs 2.5.1 **Numeric Identifier/One-dimensional barcode** and 2.5.2 **QR codes and other two-dimensional barcodes** is its cost-effectiveness and simplicity. It can be applied to the material using special inks or as a tag. The clearest disadvantage is that it is clonable, as it is relatively easy to reproduce a barcode or QR code. The threat of cloning can be mitigated through the

empowerment solution itself: the smartphone can send the identifier of the barcode or QR code to a remote application attached to the reference library, which can check the presence of duplicated identifiers and duly inform the user.

The advantage of the barcode or QR code and other overt or covert techniques in comparison to the RFID-based technique (described in paragraph 2.5.4 **Radio Frequency Identifier (RFID)**) is the cost of the token itself, even if the cost of RFID has decreased considerably in recent times. As described in [21], barcode labels cost less than USD 0.02 per label, while RFID tags are at least three times more expensive per tag. The precise cost of RFID tags varies, depending on the underlying RFID technology, but active RFID tags are usually priced between USD 20 and USD 70, whereas passive RFID tags are between USD 0.07 and USD 0.20.

The disadvantages of the barcode and QR code in comparison to RFID are [4] that a direct line of sight is requested between the reader and the code. In addition, the presence of visible light is needed with nothing obstructing the light path between them. RFID tags can be read at a distance; moreover, UHF and BAP RFID can be read at even greater distances and can be scanned much faster [21].

Regarding the different categories of users, the techniques are mostly clear and easy to understand, even if they can be complemented to increase the security of each specific class. In other words, the empowerment technique can be implemented in such a way that the smartphone provides specific data to the average citizen, and other data to brand owners, retailers and law enforcers. For example, covert data could be used for brand owners and law enforcers while only overt data is used for average citizens and retailers.

The different techniques and the different categories of users were analysed. The results of the analysis are presented in Table *1* below for the three different categories of users. The analysis was based on expert opinions and the literature (papers and reports) identified in the extensive bibliography presented at the end of this report. The analysis is differentiated for the four main techniques presented in this section (barcode and QR code are considered as one), on the basis of the metrics described in paragraph 1.3. A general paragraph is inserted if the related analysis can be applied to every technique.

In Table 1 below, 'Metrics' are those identified under paragraph 1.3, and categories of users are those identified under paragraph 1.2.

Metrics	**Law Enforcers**	**Brand Owners**	**Enterprises (especially SMEs)**
Requested resources	**Barcode and QR code** Low, because a smartphone is already equipped with NFC, a high-resolution camera and communication systems. **Physical Fingerprint Technology on visible spectrum** Low, the same as barcode and QR code (current smartphone models have high-resolution cameras). **RFID**	**Barcode and QR code** Low, if the solution is based on an extension of an existing **open-loop** track and trace infrastructure. Medium, if the solution is based on an extension of an existing **closed-loop** track and trace infrastructure. High/Very high, if a new track and trace infrastructure must be created. **Physical Fingerprint**	**Barcode and QR code** Low, because a smartphone is already equipped with NFC, a high-resolution camera and communication systems. **Physical Fingerprint Technology on visible spectrum** Low, the same as barcode and QR code (current smartphone models have high-resolution cameras). **RFID**

	Low, similar to barcode and QR code if the smartphone is equipped with an RFID reader, otherwise High. **Collection and analysis of images of the object to be authenticated** Low, the same as barcode and QR code (current smartphone models have high-resolution cameras).	**Technology on visible spectrum** Same considerations as barcode and QR code, with the additional cost of high-resolution cameras. **RFID** Same considerations as barcode and QR code with the additional cost of RFID components. **Collection and analysis of images of the object to be authenticated** Same considerations as *Physical Fingerprint Technology on visible spectrum.*	Low, similar to barcode and QR code if the smartphone is equipped with an RFID reader, otherwise High. **Collection and analysis of images of the object to be authenticated** Low, the same as barcode and QR code (current smartphone models have high-resolution cameras).
Accuracy in detecting a fake	**Barcode and QR code** Low/Medium, because of the risk of cloning. **Physical Fingerprint Technology on visible spectrum** High **RFID** Low/Medium, because of the risk of cloning, unless the RFIDs are secure (which increases the cost). **Collection and analysis of images of the object to be authenticated** Medium, because the fingerprints have not been inserted deliberately as with *Physical Fingerprint Technology on visible spectrum.*	**General** Brand owners have the advantage of inserting information or correlating information in the manufacturing/product labelling process. **Barcode and QR code** Low/Medium, because of the risk of cloning. **Physical Fingerprint Technology on visible spectrum** High **RFID** Low/Medium, because of the risk of cloning, unless the RFIDs are secure (which increases the cost). **Collection and analysis of images of the object to be authenticated** Medium, because the fingerprints have not been inserted deliberately as with *Physical Fingerprint Technology on visible spectrum.*	**Barcode and QR code** Low/Medium, because of the risk of cloning. **Physical Fingerprint Technology on visible spectrum** High **RFID** Low/Medium, because of the risk of cloning, unless the RFIDs are secure (which increases the cost). **Collection and analysis of images of the object to be authenticated** Medium, because the fingerprints have not been inserted deliberately as with *Physical Fingerprint Technology on visible spectrum.*
Need for adaptation to organisations and existing processes	**Barcode and QR code** Low, because the checking of the barcode or QR code can be easily automated. **Physical Fingerprint Technology on visible spectrum** Medium, because a procedure must be established to ensure that	**Barcode and QR code** Low, if the solution is based on an extension of an existing **open-loop** track and trace infrastructure. Medium, if the solution is based on an extension of an existing **closed-loop** track and trace infrastructure	**Barcode and QR code** Low, because the checking of the barcode or QR code can be easily automated. **Physical Fingerprint Technology on visible spectrum** Medium, because a procedure must be established to ensure that

	the correct fingerprint is collected. **RFID** Medium, because the procedure is very simple for RFID-enabled smartphones, but these specific models must be purchased as they may not be available in the mass consumer market. **Collection and analysis of images of the object to be authenticated** High, because the law enforcer must be trained to correctly collect the fingerprint, which can be different for different types of products.	High/Very high, if a new track and trace infrastructure must be created. **Physical Fingerprint Technology on visible spectrum** Same considerations as barcode and QR code with the additional cost of high-resolution cameras. **RFID** Same considerations as barcode and QR code with the additional cost of RFID components. **Collection and analysis of images of the object to be authenticated** Same considerations of *Physical Fingerprint Technology on visible spectrum.*	the correct fingerprint is collected. **RFID** Medium, because the procedure is very simple for RFID-enabled smartphones, but these models must be purchased. **Collection and analysis of images of the object to be authenticated** High, because the law enforcer must be trained to correctly collect the fingerprints, which can be different for different types of products.
Requested level of training	**Barcode and QR code** Low, because the checking of the barcode or QR code can be easily automated. **Physical Fingerprint Technology on visible spectrum** Medium, because a procedure must be established to ensure that the correct fingerprint is collected. **RFID** Low, because the procedure is very simple for RFID-enabled smartphones. **Collection and analysis of images of the object to be authenticated** High, because the law enforcers must be trained to correctly collect the fingerprints, which can be different for different types of products.	**Barcode and QR code** Low, because the checking of the barcode or QR code can be easily automated. **Physical Fingerprint Technology on visible spectrum** Medium, because a procedure must be established to ensure that the correct fingerprint is collected. **RFID** Low, because the procedure is very simple for RFID-enabled smartphones. **Collection and analysis of images of the object to be authenticated** Low/Medium, because the brand owners work with specific types of products and the collection of images can be facilitated.	**Barcode and QR code** Low, because the checking of the barcode or QR code can be easily automated. **Physical Fingerprint Technology on visible spectrum** Medium, because a procedure must be established to ensure that the correct fingerprint is collected. **RFID** Low, because the procedure is very simple for RFID-enabled smartphones. **Collection and analysis of images of the object to be authenticated** Medium/High, because the enterprises can operate with a limited set of products.
Robustness and adaptability to environmental conditions	**Barcode and QR code** High, because the checking of the barcode or QR code has been used for years in many different environmental conditions and manufacturers are able to	**Barcode and QR code** High, because the checking of the barcode or QR code has been used for years in many different environmental conditions and manufacturers are able to	**Barcode and QR code** High, because the checking of the barcode or QR code has been used for years in many different environmental conditions and manufacturers are able to

	produce environmentally robust tags and labels. **Physical Fingerprint Technology on visible spectrum** Medium, because rain or darkness can limit operability. However, fingerprints could be designed and created to be environmentally robust. **RFID** High, because the RFID is not or is slightly impacted by rain or darkness, as it uses low-frequency radio communication. **Collection and analysis of images of the object to be authenticated** Low, because rain or darkness can limit operability and the fingerprints are not designed for robustness against the environment.	produce environmentally robust tags and labels. **Physical Fingerprint Technology on visible spectrum** Medium, because rain or darkness can limit operability. However, fingerprints could be designed and created to be environmentally robust, but this can become an additional cost for the brand owner. **RFID** High, because the RFID is not or is slightly impacted by rain or darkness, as it uses low-frequency radio communication. **Collection and analysis of images of the object to be authenticated** Low, because rain or darkness can limit operability and the fingerprints are not designed for robustness against the environment.	produce environmentally robust tags and labels. **Physical Fingerprint Technology on visible spectrum** Medium, because rain or darkness can limit operability. However, fingerprints could be designed and created to be environmentally robust. **RFID** High, because the RFID is not or is slightly impacted by rain or darkness, as it uses low-frequency radio communication. **Collection and analysis of images of the object to be authenticated** Low, because rain or darkness can limit operability and the fingerprints are not designed for robustness against the environment.
Flexibility to support multiple applications	**General** As described in the rest of the report, it is possible that these techniques may be implemented using different applications and slightly different standards. This is the current situation at the time of writing this report even if current activities, such as the WCO and the IPM Connected program, can mitigate this issue. At least, this is the case for barcode and QR code based techniques. This issue is particularly relevant for law enforcers rather than other types of customers, who have to deal with a specific set of products. **Barcode and QR code** Medium, because there are currently many applications for checking barcode and QR code. Current initiatives, such as IPM Connected, can mitigate this issue (then	**General** The brand owner will likely use a specific technique and implementation for their products. As a consequence, the multi-use capability will be high because there is a single technique. **Barcode and QR code** High, because there will be only one implementation of the technique. **Physical Fingerprint Technology on visible spectrum** High, because there will be only one implementation of the technique. **RFID** High, because there will be only one implementation of the technique. **Collection and analysis of images of the object**	**General** An enterprise is usually interested only in a specific set of products. In other words, the multi-use capability is less requested than the law enforcer, but it is still needed for a set of products. As a consequence, a Medium level is suggested for all the techniques. **Barcode and QR code** Medium. **Physical Fingerprint Technology on visible spectrum** Medium. **RFID** Medium. **Collection and analysis of images of the object to be authenticated** Medium.

	the Medium level). **Physical Fingerprint Technology on visible spectrum** Low. While this technique is already offered by various companies, it is still quite fragmented, which is a considerable obstacle for law enforcers. **RFID** Low, as similar considerations for barcode and QR code apply, with the difference that as yet, IPM Connected and similar initiatives do not address RFID. **Collection and analysis of images of the object to be authenticated** Very Low, because only a few applications are on the market and the context is very fragmented or of limited distribution.	**to be authenticated** High, because there will be only one implementation of the technique.	
Upgrade capability	**Barcode and QR code** High, unless the barcode or QR code structure must be changed. **Physical Fingerprint Technology on visible spectrum** High, because the camera will be the same while only an upgrade of an application on the smartphone is needed. **RFID** High, because RFID technology is quite stable, at least for the physical layer. **Collection and analysis of images of the object to be authenticated** High, because the camera will be the same while only an upgrade of an application on the smartphone is needed.	**Barcode and QR code** High, unless the barcode or QR code structure must be changed. **Physical Fingerprint Technology on visible spectrum** High, because the camera will be the same while only an upgrade of an application on the smartphone is needed. **RFID** High, because RFID technology is quite stable, at least for the physical layer. **Collection and analysis of images of the object to be authenticated** High, because the camera will be the same while only an upgrade of an application on the smartphone is needed.	**Barcode and QR code** High, unless the barcode or QR code structure must be changed. **Physical Fingerprint Technology on visible spectrum** High, because the camera will be the same while only an upgrade of an application on the smartphone is needed. **RFID** High, because RFID technology is quite stable, at least for the physical layer. **Collection and analysis of images of the object to be authenticated** High, because the camera will be the same while only an upgrade of an application on the smartphone is needed.
Original set and deployment cost (CAPEX)	**Barcode and QR code** Medium. The smartphone must be purchased but the technology is already implemented.	**Barcode and QR code** Medium. The smartphone must be purchased but the technology is already implemented.	**Barcode and QR code** Medium. The smartphone must be purchased but the technology is already implemented.

	Physical Fingerprint Technology on visible spectrum Medium. The smartphone must be purchased. **RFID** Medium/High. A smartphone with an RFID reader must be purchased. **Collection and analysis of images of the object to be authenticated** Medium. The smartphone must be purchased.	**Physical Fingerprint Technology on visible spectrum** Medium. The smartphone must be purchased. **RFID** Medium/High. A smartphone with an RFID reader must be purchased. **Collection and analysis of images of the object to be authenticated** Medium. The smartphone must be purchased.	**Physical Fingerprint Technology on visible spectrum** Medium. The smartphone must be purchased. **RFID** Medium/High. A smartphone with an RFID reader must be purchased. **Collection and analysis of images of the object to be authenticated** Medium. The smartphone must be purchased.
Operational Cost (OPEX)	**Barcode and QR code** Low. **Physical Fingerprint Technology on visible spectrum** Low. **RFID** Low. **Collection and analysis of images of the object to be authenticated** Low.	**Barcode and QR code** Low. **Physical Fingerprint Technology on visible spectrum** Low. **RFID** Low. **Collection and analysis of images of the object to be authenticated** Low.	**Barcode and QR code** Low. **Physical Fingerprint Technology on visible spectrum** Low. **RFID** Low. **Collection and analysis of images of the object to be authenticated** Low.
Market and standardisation support	**Barcode and QR code** Medium. While there are many applications on the market, a common standard must still be defined even if there are available drafts. **Physical Fingerprint Technology on visible spectrum** Low. There are not many applications on the market. **RFID** Medium. While there are many applications on the market, a common standard must still be defined even if there are available drafts. **Collection and analysis of images of the object to be authenticated** Very Low, as this technique is not widely deployed.	**Barcode and QR code** High. Many brand owners have built and deployed their own version of the technique. **Physical Fingerprint Technology on visible spectrum** Medium. There are not many applications on the market but some brand owners have implemented it. **RFID** Medium/High. Many brand owners have built and deployed their own version of the technique even if it less deployed than barcode and QR code because of the costs. **Collection and analysis of images of the object to be authenticated** Very Low, as this technique is not widely deployed.	**Barcode and QR code** Medium. While there are many applications on the market, a common standard must still be defined even if there are available drafts. **Physical Fingerprint Technology on visible spectrum** Low. There are not many applications on the market. **RFID** Medium. While there are many applications on the market, a common standard must still be defined even if there are available drafts. **Collection and analysis of images of the object to be authenticated** Very Low, as this technique is not widely deployed.
Interoperability with	**General**	**General**	**General**

existing open tools	Law enforcers can use existing activities, such as IPM Connected, to bridge the techniques to ICT systems already deployed. For techniques already deployed, the level of interoperability can be high, while it is low for techniques that have limited deployment in the market. **Barcode and QR code** Medium **Physical Fingerprint Technology on visible spectrum** Low **RFID** Low/Medium **Collection and analysis of images of the object to be authenticated** Very Low	Brand owners have usually designed and deployed track and trace solutions to support their production and distribution chain. Then, they have a high degree of interoperability because the techniques used for fighting against counterfeiting are an evolution of the existing systems. **Barcode and QR code** Very High **Physical Fingerprint Technology on visible spectrum** Medium **RFID** Medium **Collection and analysis of images of the object to be authenticated** Low	Enterprises must build up a new system in many cases, even if they already have distribution channels with suppliers. As a consequence, the degree of interoperability is less for the brand owners but slightly higher for the law enforcers, at least for some techniques. **Barcode and QR code** Medium/High **Physical Fingerprint Technology on visible spectrum** Low/Medium **RFID** Medium **Collection and analysis of images of the object to be authenticated** Very Low

Table 1. Comparison of the empowerment techniques based on the smartphone

To provide a quantitative as well as the qualitative analysis summarised in Table 1 above, we have adopted a scoring system to calculate the overall scope for each technique for the different categories of users.

The scoring system assigns the following values:

Very Low	2
Low	4
Medium	6
High	8
Very High	10

We note that some metrics are positive: a high evaluation is an advantage for the technique, while some metrics are negative and a high evaluation is a disadvantage for the technique. In the scoring, the negative metrics will be subtracted from the overall score.

The quantitative summary, based on Table 1, is shown in Table 2 below:

In the table, the ‘Metrics’ are those identified under paragraph 1.3, and categories of users are those identified under paragraph 1.2.

Metrics	**Law Enforcers**	**Brand Owners**	**Enterprises (especially SMEs)**
Barcode and QR code	29	33	30

Physical Fingerprint Technology on visible spectrum	20	25	23
RFID	23	26	25
Collection and analysis of images of the object to be authenticated	6	15	9

Table 2. Quantitative analysis

From the quantitative analysis, we can see that barcode and QR code is the clear winner among the techniques for all the categories of users with RFID as a second technique. The collection and analysis of images still require further research.

Barcode/QR code is the most effective technique among the ones using the smartphone for all categories of users.

2.6 Findings on empowerment for fight against IP infringing using smartphones

Techniques using smartphones have now reached maturity and they can be both cost-effective and highly accurate in identifying and authenticating a product. These techniques can be applied by the brand owner as part of the product itself, or they can be applied to the product depending on the feasibility of applying intrinsic features.

With its high-resolution camera and wireless connectivity, the smartphone also has the capability to support the various techniques.

One potential issue is the variety of technical solutions present on the market, which requires a standardisation effort to avoid complex validation procedures by the various categories of users, which may limit the validity of these techniques. For example, a law enforcer may be obliged to use many different smartphone applications for each technique or brand.

This aspect alone makes the option of using the EUIPO's EDB as the reference library in the EU even more relevant, especially if accompanied with a process at European level to establish a common standard. In particular, the standard should define the generation of unique security identifiers and the protocols between the smartphone and the reference library (see Chapter 5).

3 Use of a Specific Portable Device, Other than a Smartphone

3.1 Introduction

This section analyses the techniques used to empower the user using portable devices, which can be used in the field to identify and distinguish a genuine product from a counterfeit one. In particular, we investigate the adoption in the field of forensic techniques, which were previously only possible in specialised labs but are now accessible using portable devices, with some limitations.

A portable device, that is to say, an electronic device, is equipped with sensors, a processing platform and a display. Simpler devices, which can be used in the field, are discussed in the following section.

In this section, we also analyse plug-in devices, which can be connected to smartphones. The reason why these devices are addressed here and not in the previous section is that a user must still acquire them and carry them with them, which is justified for specific categories of users (e.g. law enforcers, enterprises) but not all. RFID readers are an exception to this rule, because smartphones already partially support them and the trend is to achieve full support in a few years time.

The status provided in this section is at the moment of writing this report (January 2017). As technology progresses, new devices appear on the market.

The main categories identified are:

1) devices for the collection of radio frequency signals in space
2) portable spectrometers
3) augmentation devices for smartphones or other IoT devices
4) simple devices for visual augmentation.

3.2 Devices for the collection of radio frequency signals in space

The technique is based on the concept that electronic circuits, when powered, emit radio frequency emissions, which are intrinsically linked to the physical structure of the circuit. Using a parallel from biology, the RF emissions can be linked to the DNA of the electronic circuit or component.

The idea is that electronic circuits and mobile devices that are IP infringing have specific RF emissions, which distinguish them from genuine equipment. This is due to the fact that the worst materials (i.e. cheap substandard components) or manufacturing practices are used to produce the electronic equipment at less cost than the genuine equipment. This has been reported by many sources, such as [23][24].

There are various examples of the application of this technique from the literature. For example, [25] shows how RF emissions can be used to uniquely identify integrated circuits. Similarly, [26] has shown the specific identity of GSM phones, which can be detected on the basis of their RF emissions, not only for different models but also for different smartphones within the same model (e.g. smartphones with different serial numbers).

Intrinsic features can also be inserted in the electronic device in the manufacturing process. One example is the Physical Unclonable Functions (PUF), which has also reached market maturity at this stage, as they are provided.

The identification of electronic devices, including consumer mass products such as smartphones or tablets, through radio frequency emissions was still a forensic activity until recently. The reasons were based on a) the cost of the radio frequency systems to collect the RF signals in the air, b) the complexity of the algorithms, which was so demanding that specialised hardware was needed and c) the training needed to execute such algorithms.

This context has changed with the introduction of new radio frequency front ends and signal processing devices, which have a cost of around EUR 20 (e.g. RTL-SDR) and they can be easily plugged into a smartphone or cost-effective portable system. The processing power of the modern smartphone is such that the execution of sophisticated algorithms can be executed in a matter of seconds for the signal analysis. The RTL-SDR operates in various frequency ranges, which are suitable for the most common wireless communication standards and frequency bands of a mobile device.

Note that RFIDs are also electronic components. Beyond the ID information, radio frequency signals can also be analysed to improve signal identification. In other words, the cloning of the identifier (the ID) in the RFID can be prevented by the analysis of the radio frequency signal.

The adoption of radio frequency analysis as a method to fight against counterfeit products is similar to other methods: it is based on the creation of a reference library, which stores the radio frequency signals of the electronic devices, which can be collected in the manufacturing process before distribution. For example, RF signals can be collected in the standard testing phase, where the transmission or reception capabilities of the smartphone are tested, thus avoiding an additional step in the manufacturing process.

The following elements can be part of this technique:

1) **A remote database**. A back-end database (e.g. cloud computing) should be created with all the fingerprints of RF emissions of the goods to be checked for IP infringing.

2) **Implementation of the algorithms**. Sophisticated algorithms for pattern matching should be implemented. The algorithms should be optimised for the type of product.

3) **Fingerprint collection**. Fingerprints should be collected for each type of product produced by a manufacturer (e.g. electronic circuit, smartphone).

4) **Radio frequency receivers**. Mobile devices (e.g. smartphones) of the user should be equipped with radio frequency receivers, to collect the RF sample at short range in a wide range of frequencies.

5) **Data connectivity**. Users should have access to high-speed wireless data links to support the upload of RF fingerprinting to the central cloud, even if some pre-processing can be done.

To summarise, whereas this technique is still in the research or prototype phase, it is still possible to devise cost-effective plug-ins and simple algorithm processes.

3.3 Portable spectrometers

Various references have described the applicability of portable spectrometers to the fight against counterfeiting, especially in the pharmaceutical sector. For example, [27] and [28] have reported in their findings on portable spectrometers the identification of counterfeit

drugs. Here, we mean various types of spectrometers from Raman Spectroscopy to Near Infrared Spectroscopy (NIRS). See report JRC98181 for a detailed description of spectroscopy techniques and their application to the fight against counterfeiting. In particular, [28] has pointed out that 'Raman spectroscopy has rapidly evolved over the past 10 years and offers many benefits that include smaller, faster, and [more] portable units that can be very advantageous especially when working to verify counterfeit medicine. This technology is here to stay, and although it brings many advantages, users need to be mindful that the use of portable instruments for counterfeit verification is not without limitations. The degree of uncertainty in the results can be due to spectral features such as S/N, fluorescence, sample properties, or other random variability of the spectral data. Users should consider using more than 1 correlation method and/or spectral technique for product authentication when the result generated by the Raman portable instrument is close to the threshold value (i.e. a p-value of 0.05). The results are not necessarily trustworthy until further verification is performed'.

In a similar way, [27] has stated that 'Spectrometers have evolved after having been around for about 50 years now. But, when it was first invented and put together, they were all huge spectrometers that would actually fill up an entire room, believe it or not. And now it has gotten smaller and smaller and smaller to where now spectrometers are the size of a clip-on to your iPhone. In fact, people are now developing apps to really control and maintain and even detect a counterfeit, just by using even your iPhone. Because the iPhone camera flash is becoming the light source for the spectrometer', and 'In fact, U.S. Customs and Border Control agencies, along with the FDA, are putting the spectrometers in place everywhere — even in airports where people are trying to smuggle pharmaceutical counterfeits. It is becoming more and more of a well-accepted technology. Even 5-6 years ago when we started, it was not well-accepted in the industry. But, now it's been well-accepted within all the regulatory bodies in and outside of the U.S'.

Furthermore, these views have been confirmed by other sources (i.e. [29]), which reported that 'Our new method is built on modified LSLS algorithm and PCA with very small training set. This assay proves to be a successful high-throughput screening approach for hypoglycemic, which involves three types of counterfeit drugs. Firstly, deliberate and time-consuming collection of thousands of authentic drugs, construction and updating of qualitative or quantitative model for every kind of drug could be evaded. Secondly, after all the standard spectra of the commonly-counterfeited APIs have been stored in the spectral database, whichever drug(s) could be calculated promptly to discriminate whether it is counterfeited by any database-stored API(s). Although, the use of Raman spectroscopy for drug detection is not a good choice due to the high energy of the light source and the difficulties in the measurements'. The reference by [29] points to some limitations to the accuracy of portable spectrometers in comparison to spectrometers used in forensic labs, which is understandable considering the different prices and capabilities of the equipment. Nevertheless, the level of accuracy is adequate for prescreening, which has already been confirmed by previous references [30].

To summarise, portable spectrometers are now available on the market and various companies offer cost-effective equipment, which can be used by various categories of users. While this may not be applicable to the category of the average citizen, law enforcers, enterprise and retailers/distributors can use portable spectrometers to prescreen counterfeit medicines and other materials.

Apart from the decrease in accuracy in comparison to a forensic lab, the limitation of this empowerment technique is its specificity for the pharmaceutical sector and for specific types of medicines. In addition, a similar framework to the other techniques must be put in place, with the following components.

1) **A remote database**. A back-end database (e.g. cloud computing) should be created with the features of the goods (e.g. medicines).

2) **Implementation of the algorithms**. Sophisticated algorithms for pattern matching should be implemented.

3) **Fingerprint collection**. The features of the product (e.g. medicine) should be collected and recorded in the manufacturing phase.

4) **Portable spectrometers**. Portable spectrometers are needed to collect the data in the field.

5) **Data connectivity**. Users should have access to high-speed wireless data links to support the upload of collected data to the central cloud, even if some preprocessing can be done.

3.4 Augmentation devices for smartphones or other IoT devices

Other augmentation devices are also available for smartphones. One of the most common and simple is a USB magnifier, which can be connected to a smartphone or computer. This simple tool can be used to improve a user's visual capabilities to inspect a potentially counterfeit good.

The application of USB microscopes, which provide the image directly to a computer, has been mentioned in [31] specifically for the fight against counterfeit circuits. The USB microscope is fairly inexpensive. For the detection of counterfeit parts, a microscope with at least 30X magnification is recommended. It is also important that the user has a camera built into their microscope [32].

More powerful tools have been researched and developed by DARPA, as described in [33]. One of DARPA's contractors has developed and deployed an Advanced Scanning Optical Microscope that can scan integrated circuits by using an extremely narrow infrared laser beam, to probe microelectronic circuits at nanometre levels, revealing information about chip construction as well as the function of circuits at transistor level.

Another category of equipment is based on reality augmentation devices, such as Google Glass. An example of the application of Google Glass in the fight against counterfeiting is described in [40].

3.5 Use of simple devices

In this section, we describe the availability of simple devices, which have appeared recently on the market. The term 'simple devices' refers to cost-effective tools, which can be used in a simple way (e.g. no training or very basic training) and which are not present in the previous categories (e.g. smartphone or portable spectrometers).

Examples of 'simple devices' are:

1) Ultraviolet light detectors, which shine ultraviolet light against the surface of a product or a package to highlight any embedded features.

2) Polarised filters implemented on a simple strip, which can be used to highlight features embedded in a material (e.g. textile) or a label. In other words, a hidden image that becomes visible only through a special polariser. There are various examples on the market of available products using this technique, such as Latentogram® by ATB GROUP or from research [34].

3) Thin-layer chromatography, a chromatography technique used to separate non-volatile mixtures [35], which can be used in the area of medicine. Thin-layer chromatography is performed on a sheet of glass, plastic, or aluminum foil, which is coated with a thin layer of adsorbent material, usually silica gel, aluminum oxide, or cellulose. It can be employed for the identification of drug substances, the estimation of drug substance content and the detection of related substances that could be regarded as impurities. Note that thin-layer chromatography can only be applied where a chemical reaction is used to identify the product (e.g. medicine sample).

Other techniques can be developed in the future, so the previous list is not exhaustive.

All these techniques require very simple, lightweight, inexpensive tools and a low level of training (with the exception of thin-layer chromatography). While technique 3 is for specific types of goods where the chemical composition of the product must be assessed (e.g. pharmaceutical products), the first two techniques can be applied directly to labels applied to goods and packages.

The main advantages of these techniques (especially 1 and 2) are simplicity, low cost, no need for remote connectivity, a low-level need for training and portability (a strip to apply Latentogram is only a few centimetres long and weighs ten grams). The potential disadvantages are that they can be used mostly to authenticate rather than identify goods or to obtain additional information from a remote reference library. Nevertheless, they can be an effective instrument in the fight against counterfeiting.

3.6 Findings on empowerment using specific portable devices, other than a smartphone

Different types of analysis apply to the different categories presented in the previous sections.

1) Devices for the collection of radio frequency signals in space.
2) Portable spectrometers.
3) Augmentation devices for smartphones or other IoT devices.
4) Simple devices.

The first category is still in the research or prototype phase, even if this is in fact possible with the technologies currently available. Nevertheless, its market deployment has still not happened at the time of writing this report. For some categories of user, some training is also required to capture radio frequency signals appropriately in space. A strong limitation of this technique is that it can be used only for a specific category of goods.

Portable spectrometers became available on the market and some categories of users, such as law enforcers or brand owners, are able to use them to distinguish between valid and counterfeit goods. While their market availability is certainly better than for the first category, some training is still needed to analyse goods effectively. The need for training somewhat limits the applicability of this technique to trained law enforcers and brand owners, who

presumably are already familiar with it. Portable spectrometers can be quite accurate for very specific categories of goods, but they are inappropriate for many other categories.

The third category is the most appropriate when the technology is relatively simple to use, as in the case of a USB microscope or when the device itself can automate identification, as in the case of Google Glass. The evolution of IoT and augmented reality devices can undeniably automate solutions for the fight against counterfeiting and this is an important trend to consider.

The fourth category is quite simple to adopt and can be used for a large variety of categories, including packaged goods. The limitation is that it mostly provides the identification and authentication of goods rather than detailed information, as it does not connect to a reference library and associated database. For example, tax information would be difficult to implement. Nevertheless, this category of techniques can be a simple and valid tool for authenticating goods.

The analysis presented above is summarised in Table 3 below.

In the table, 'Metrics' are those identified under paragraph 1.3, and categories of user are those identified under paragraph 1.2.

Metric	Law Enforcers	Brand Owners	Enterprises (especially SMEs)
Requested resources	**Devices for the collection of radio frequency signals in space.** High, because even low-cost sensors/receivers cost hundreds of dollars. **Portable spectrometers** Medium/High. Even if the prices have dropped considerably, portable spectrometers are still relatively expensive. **Augmentation devices for smartphones or other IoT devices** Low/Medium, depending on the augmentation device. **Use of simple devices** Low/Medium, because law enforcers may need to equip themselves with many different systems, even if they are low-cost on a single basis.	**Devices for the collection of radio frequency signals in space.** High, because even low-cost sensors/receivers cost hundreds of dollars. **Portable spectrometers** Medium/High. Even if the prices have dropped considerably, portable spectrometers are still relatively expensive. **Augmentation devices for smartphones or other IoT devices** Low/Medium, depending on the augmentation device. **Use of simple devices** Low, because brand owners must equip themselves with only one device.	**Devices for the collection of radio frequency signals in space.** High, because even low-cost sensors/receivers cost hundreds of dollars. **Portable spectrometers** Medium/High. Even if the prices have dropped considerably, portable spectrometers are still relatively expensive. **Augmentation devices for smartphones or other IoT devices** Low/Medium, depending on the augmentation device. **Use of simple devices** Low/Medium, because enterprises may need to equip themselves with different systems, even if they are low-cost on a single basis.
Accuracy in detecting a fake	**Devices for the collection of radio frequency signals in space.** Low/Medium. Accuracy can be low depending on the quality of the used receiver.	**Devices for the collection of radio frequency signals in space.** Low/Medium. Accuracy can be low depending on the quality of the used receiver.	**Devices for the collection of radio frequency signals in space.** Low/Medium. Accuracy can be low depending on the quality of the used receiver.

	Portable spectrometers Medium/High accuracy has been reported. **Augmentation devices for smartphones or other IoT devices** Medium. Depends on the augmentation device. **Use of simple devices** Medium/High accuracy has been reported.	**Portable spectrometers** Medium/High accuracy has been reported. **Augmentation devices for smartphones or other IoT devices** Medium. Depends on the augmentation device. **Use of simple devices** Medium/High accuracy has been reported.	**Portable spectrometers** Medium/High accuracy has been reported. **Augmentation devices for smartphones or other IoT devices** Medium. Depends on the augmentation device. **Use of simple devices** Medium/High accuracy has been reported.
Need for adaptation to organisations and existing processes	**Devices for the collection of radio frequency signals in space.** Very Low, because no equivalent system is in place. **Portable spectrometers** Low, because law enforcers have used portable spectrometers only on limited occasions. **Augmentation devices for smartphones or other IoT devices** Medium. Depends on the augmentation device. **Use of simple devices** High, because these techniques do not require a complex infrastructure to be set up.	**Devices for the collection of radio frequency signals in space.** Very Low, because no equivalent system is in place. **Portable spectrometers** Low/Medium, because brand owners have used portable spectrometers only on limited occasions, apart from some specific domains such as the pharma industry. **Augmentation devices for smartphones or other IoT devices** Medium. Depends on the augmentation device. **Use of simple devices** High, because these techniques do not require a complex infrastructure to be set up.	**Devices for the collection of radio frequency signals in space.** Very Low, because no equivalent system is in place. **Portable spectrometers** Low, because enterprises have used portable spectrometers only on limited occasions. **Augmentation devices for smartphones or other IoT devices** Medium. Depends on the augmentation device. **Use of simple devices** High, because these techniques do not require a complex infrastructure to be set up.
Requested level of training	**Devices for the collection of radio frequency signals in space.** Very high, because they are completely new systems and techniques. **Portable spectrometers** High, because they are a new technique for law enforcers. **Augmentation devices for smartphones or other IoT devices** Medium. Depends on the augmentation device. **Use of simple devices** Low, because they are quite simple to use.	**Devices for the collection of radio frequency signals in space.** High, because they are completely new systems and techniques, even if a brand owner would have specific knowledge to facilitate the training process. **Portable spectrometers** Medium/High, because they are a new technique even if a brand owner would have specific knowledge to facilitate the training process. **Augmentation devices for smartphones or other IoT devices**	**Devices for the collection of radio frequency signals in space.** High, because they are completely new systems and techniques, even if an enterprise working in this field would have specific knowledge to facilitate the training process. **Portable spectrometers** Medium/High, because they are a new technique even if an enterprise working in the field would have specific knowledge to facilitate the training process.

		Medium. Depends on the augmentation device. **Use of simple devices** Low, because they are quite simple to use.	**Augmentation devices for smartphones or other IoT devices** Medium. Depends on the augmentation device. **Use of simple devices** Low, because they are quite simple to use.
Robustness and adaptability to environmental conditions	**Devices for the collection of radio frequency signals in space.** Very high, because they are not dependent on rain or darkness. **Portable spectrometers** Medium/High, because they are usually robust against environmental conditions. **Augmentation devices for smartphones or other IoT devices** Medium. Depends on the augmentation device. **Use of simple devices** Low/Medium, because they are of limited use in darkness.	**Devices for the collection of radio frequency signals in space.** Very high, because they are not dependent on rain or darkness. **Portable spectrometers** Medium/High, because they are usually robust against environmental conditions. **Augmentation devices for smartphones or other IoT devices** Medium. Depends on the augmentation device. **Use of simple devices** Low/Medium, because they are of limited use in darkness.	**Devices for the collection of radio frequency signals in space.** Very high, because they are not dependent on rain or darkness. **Portable spectrometers** Medium/High, because they are usually robust against environmental conditions. **Augmentation devices for smartphones or other IoT devices** Medium. Depends on the augmentation device. **Use of simple devices** Low/Medium, because they are of limited use in darkness.
Flexibility to support multiple applications	**Devices for the collection of radio frequency signals in space.** Medium, if the sensor device can support different wireless standards and frequency bands. **Portable spectrometers** Medium, because they can be used for different types of products. **Augmentation devices for smartphones or other IoT devices** Medium. Depends on the augmentation device. **Use of simple devices** Low/Medium, because different devices must be used unless a common standard is defined.	**Devices for the collection of radio frequency signals in space.** Medium, if the sensor device can support different wireless standards and frequency bands. **Portable spectrometers** Medium, because they can be used for different types of products. **Augmentation devices for smartphones or other IoT devices** Medium. Depends on the augmentation device. **Use of simple devices** High, because a brand owner will use only one type of device.	**Devices for the collection of radio frequency signals in space.** Medium, if the sensor device can support different wireless standards and frequency bands. **Portable spectrometers** Medium, because they can be used for different types of products. **Augmentation devices for smartphones or other IoT devices** Medium. Depends on the augmentation device. **Use of simple devices** Medium, because different devices must be used unless a common standard is defined.
Upgrade capability	**Devices for the collection of radio frequency signals in space.** Medium, if the sensor device can support	**Devices for the collection of radio frequency signals in space.** Medium, if the sensor device can support	**Devices for the collection of radio frequency signals in space.** Medium, if the sensor device can support

	different wireless standards and frequency bands. **Portable spectrometers** Medium, because they can be used for different types of products. **Augmentation devices for smartphones or other IoT devices** Medium. Depends on the augmentation device. **Use of simple devices** Low/Medium, because the device must be upgraded.	different wireless standards and frequency bands. **Portable spectrometers** Medium, because they can be used for different types of products. **Augmentation devices for smartphones or other IoT devices** Medium. Depends on the augmentation device. **Use of simple devices** Low/Medium, because the device must be upgraded.	different wireless standards and frequency bands. **Portable spectrometers** Medium, because they can be used for different types of products. **Augmentation devices for smartphones or other IoT devices** Medium. Depends on the augmentation device. **Use of simple devices** Low/Medium, because the device must be upgraded.
Original set and deployment cost (CAPEX)	**Devices for the collection of radio frequency signals in space.** High, because a significant number of receivers must be purchased and deployed. **Portable spectrometers** High, because a significant number of spectrometers must be purchased and deployed. **Augmentation devices for smartphones or other IoT devices** Medium. Depends on the augmentation device. **Use of simple devices** Very Low, because the devices have a very low cost.	**Devices for the collection of radio frequency signals in space.** High, because a significant number of receivers must be purchased and deployed. **Portable spectrometers** High, because a significant number of spectrometers must be purchased and deployed. **Augmentation devices for smartphones or other IoT devices** Medium. Depends on the augmentation device. **Use of simple devices** Very Low, because the devices have a very low cost.	**Devices for the collection of radio frequency signals in space.** High, because a significant number of receivers must be purchased and deployed. **Portable spectrometers** High, because a significant number of spectrometers must be purchased and deployed. **Augmentation devices for smartphones or other IoT devices** Medium. Depends on the augmentation device. **Use of simple devices** Very Low, because the devices have a very low cost.
Operational cost (OPEX)	**Devices for the collection of radio frequency signals in space.** Medium, if upgrades are needed. **Portable spectrometers** Medium, in case upgrades are needed. **Augmentation devices for smartphones or other IoT devices** Low. Depends on the augmentation device. **Use of simple devices** Very Low, because the devices have a very low cost.	**Devices for the collection of radio frequency signals in space.** Medium, if upgrades are needed. **Portable spectrometers** Medium, in case upgrades are needed. **Augmentation devices for smartphones or other IoT devices** Low. Depends on the augmentation device. **Use of simple devices** Very Low, because the devices have a very low cost.	**Devices for the collection of radio frequency signals in space.** Medium, if upgrades are needed. **Portable spectrometers** Medium, in case upgrades are needed. **Augmentation devices for smartphones or other IoT devices** Low. Depends on the augmentation device. **Use of simple devices** Very Low, because the devices have a very low cost.

Market and standardisation support	**Devices for the collection of radio frequency signals in space** Very low support by the market, as this technique has limited deployment. **Portable spectrometers** Low/Medium, because portable spectrometers are available on the market even if not particularly for anti-counterfeiting applications. **Augmentation devices for smartphones or other IoT devices** Low. Depends on the augmentation device. **Use of simple devices** Medium, because these devices have a still limited market deployment even if the costs are very low.	**Devices for the collection of radio frequency signals in space** Very low support by the market, as this technique has limited deployment. **Portable spectrometers** Low/Medium, because portable spectrometers are available on the market even if not particularly for anti-counterfeiting applications. **Augmentation devices for smartphones or other IoT devices** Low. Depends on the augmentation device. **Use of simple devices** Medium, because these devices have a still limited market deployment even if the costs are very low.	**Devices for the collection of radio frequency signals in space** Very low support by the market, as this technique has limited deployment. **Portable spectrometers** Low/Medium, because portable spectrometers are available on the market even if not particularly for anti-counterfeiting applications. **Augmentation devices for smartphones or other IoT devices** Low. Depends on the augmentation device. **Use of simple devices** Medium, because these devices have a still limited market deployment even if the costs are very low.
Interoperability with existing open tools	**Devices for the collection of radio frequency signals in space.** Very Low, because these devices use different systems and reference libraries from the existing system. **Portable spectrometers** Very Low, because these devices use different systems and reference libraries from the existing system. **Augmentation devices for smartphones or other IoT devices** Medium, because some of the augmentation techniques are similar to the existing ones (visual inspection). **Use of simple devices** Medium/High, because techniques based on polarised light are still a form of visual inspection.	**Devices for the collection of radio frequency signals in space.** Very Low, because these devices use different systems and reference libraries from the existing system. **Portable spectrometers** Very Low, because these devices use different systems and reference libraries from the existing system. **Augmentation devices for smartphones or other IoT devices** Medium, because some of the augmentation techniques are similar to the existing ones (visual inspection). **Use of simple devices** Medium/High, because techniques based on polarised light are still a form of visual inspection.	**Devices for the collection of radio frequency signals in space.** Very Low, because these devices use different systems and reference libraries from the existing system. **Portable spectrometers** Very Low, because these devices use different systems and reference libraries from the existing system. **Augmentation devices for smartphones or other IoT devices** Medium, because some of the augmentation techniques are similar to the existing ones (visual inspection). **Use of simple devices** Medium/High, because techniques based on polarised light are still a form of visual inspection.

Table 3. Summary of the analysis

To provide a quantitative as well as the qualitative analysis summarised in Table *3* above, we have adopted a scoring system to calculate the overall scope for each of the techniques for the different categories of user.

The scoring system assigns the following values:

Very Low	2
Low	4
Medium	6
High	8
Very High	10

We note that some metrics are positive: a high evaluation is an advantage for the technique, while some metrics are negative and a high evaluation is a disadvantage for the technique. In the scoring, the negative metrics will be subtracted from the overall score.

The quantitative summary, based on Table *3*, is shown in Table *4* below:

In the following table, 'Metrics' are those identified under paragraph 1.3, and categories of users are those identified under paragraph 1.2.

	Law Enforcers	**Brand Owners**	**Enterprises (especially SMEs)**
Devices for the collection of Radio Frequency signal in space.	2	3	3
Portable spectrometers	8	10	9
Augmentation devices for smartphones or other IoT devices	18	18	18
Use of simple devices	30	34	31

Table 4. Quantitative analysis

From the quantitative analysis, we can see that the use of simple devices is the clear winner among the techniques and its score is comparable to the barcode and QR code technique from the previous section.

The use of simple devices (e.g. polarised light) is the most effective technique among the techniques using specific portable devices, other than a smartphone.

4 Issues and Challenges for Empowerment

4.1 Privacy aspects

This section addresses the problem of a consumer's privacy in the context of empowerment. This issue potentially impacts on only the average citizen category, as the other categories will use empowerment techniques as part of their professional duties. By contrast, the average citizen may be rightfully worried that empowerment techniques could provide a remote application with their personal data when checking whether goods are counterfeit.

Privacy aspects can be addressed easily, using the two privacy protection techniques that follow in the design of the application on the smartphone.

1. Application of anonymisation technology, before sending data to the remote application to check if goods are counterfeit. The term 'anonymisation' refers to the process to render the data sent to the remote application 'anonymous' as regards the consumer's identity. For example, the smartphone user's identity, or other identifying data (e.g. location), is removed from the set of transmitted data.

2. Use of informed consent. In this instance, the consumer accepts that the transmitted data contains personal information through informed consent, which is registered electronically on the smartphone and sent together with the application data. The consumer can provide informed consent for various reasons. For example, the application developed by uFaker, gives prizes to consumers who report a counterfeit item [14]. The consumer can provide identification information voluntarily.

More sophisticated Privacy Enhancing Technologies (PET) can be used to protect the privacy rights of citizens, but these technologies come at a cost.

The economics related to the deployment of PET or more sophisticated forms of informed consent can undoubtedly be an obstacle to the deployment of empowerment techniques in the fight against counterfeiting. In this instance, the recommendation is to adopt simple PET that are already available on the market for the design of the application to empower the consumer. We reiterate that the protection of privacy rights applies to only one category of consumer.

4.2 Market fragmentation

This report and other reports on technologies for the fight against counterfeiting have clearly demonstrated that there are many empowerment technologies on the market. Such technologies can use the smartphone, which is today a consumer mass market device (and whose cost will decrease even further in the future), or other devices that are either simpler or more sophisticated. We claim that the new set of technologies and applications can support the fight against counterfeiting in a more effective way than in previous years.

Beyond these positive developments, one significant issue is the variety of techniques in the different domains and sectors, which can become a hurdle for the users that belong to the professional categories, such as law enforcers and retailers or distributors.

While brand owners and producers work in their specific sectors and may adopt only one or two empowerment techniques, law enforcers have to evaluate many different types of goods in their daily activities. The availability of many different empowerment techniques and applications may become a hindrance rather than an effective supporting tool, because law

enforcers will have to use a separate technique for different types of goods and even different types of brands. It is easy to imagine that such an approach is impractical and may have a negative impact on the deployment of empowerment techniques in the law enforcer community and in other categories as well (e.g. retailers and distributors). The average citizen can also be adversely affected by the availability of empowerment techniques, but for this category, the adoption of these techniques is on a voluntary basis rather than required by their professional activities. Thus, it can be less relevant.

Actions must be taken to support law enforcers and retailers or distributors to overcome these issues. Various approaches are possible.

1) A common standard for identification and authentication is defined for brands belonging to the same sector or across different sectors. Then, applications are developed on the basis of this standard in such a way that a single application is able to evaluate goods of different brands in a specific sector. While this is not an easy task, there are already standardisation efforts in place like the one described in section 2.3.1 (e.g., CODENTIFY), which can be a valid basis for further development.

2) Foster a collaborative cooperation from law enforcement authorities, EU institutions, and industry associations to use the EDB as the reference library in the EU, so that convergence efforts are concentrated in one single library. If accompanied by (a) developments intended to enable law enforcers and brand owners to use smartphones to access the information contained in the database securely; and (b) a standardisation process at EU level; this solution has the potential to step up the fight against counterfeiting in the EU significantly. Furthermore, this could be achieved at a reduced cost for both law enforcement authorities and brand owners, as the main investment would be undertaken by the EUIPO.

4.3 Training

The various empowerment techniques presented in this report do require some level of training, which can range from low in the case of smartphones reading a barcode, to relatively high in the case of portable spectrometers.

Training and knowledge on how to use each empowerment technique are important elements in their successful deployment, as a lack of training can reduce accuracy in identifying goods. A lack of accuracy and the consequent frustration from users when using the techniques could lead very quickly to a complete rejection of the empowerment technique. Training should be provided by the companies (e.g. brand owners) or technological implementers of the technique.

The operational effort needed to develop training practices for empowerment solutions can be considerable and it is preferable that the empowerment techniques develop automatic support mechanisms. For example, a wizard or an automated sequence of steps is implemented to guide the user in the proper acquisition of a product’s data.

5 Conclusions and suggestions

In this section, some suggestions are given on possible steps to take at EU level in order to ensure the best use of available identified technologies in the fight against counterfeiting by law enforcers and business, based on the analysis provided in the previous paragraphs.

5.1 Standardisation of the authentication technique for empowering the user

The presence of many technological solutions on the market to empower users in the fight against counterfeiting and IPR infringing using smartphones confirms that the techniques described in paragraphs 2.3.1 **Reference library created by a brand owner during the manufacturing process**and 2.3.2 **Reference library created by a third party working with a brand owner** are now mature and cost-efficient. However, the presence of many different solutions creates an obstacle to the deployment of techniques, as the user needs to use many different applications for different sectors and even different brands in the same sector. It is suggested that every effort is made to further develop the reference library at the EUIPO (the EDB) and to initiate a standardisation activity that selects and develops a single standard to support goods' authentication and the tracking and tracing of goods. Starting points for the definition of the standard could be CODENTIFY by DCTA (Digital Coding and Tracking Association) or the serialisation and tracking solution, which is being defined in the pharmaceutical industry on the basis of Directive (EU) 2016/161 (see the German pilot project in [38]). The ISO standardisation technical committee ISO/TC 246 anti-counterfeiting tools may be involved.

Suggestion 1): a common standard to empower the user for goods' authentication through the smartphone should be developed. In particular, the standard should define the generation of unique secured identifiers and the protocols between the smartphone and the remote reference library (EUIPO EDB).

5.2 Creation of an expert group on the empowerment of the user

Various technologies are created every year in the market to identify and authenticate goods through the smartphone and other portable instruments. Each technique can be appropriate for specific domains. An expert group should be created to investigate and analyse annually the new solutions on the market and evaluate the applicability in various domains. This activity can be linked to the standardisation activity described in the previous recommendation in paragraph 5.1. Furthermore, the group could advise the EUIPO on the integration in its EDB of the most efficient techniques, thus stepping up the EU enforcers' capacity to fight against counterfeiting.

The expert group should consist of manufacturers, retailers, distributors, law enforcers, developers of anti-counterfeit solutions, government representatives and consumer associations.

Suggestion 2): create an expert group for the analysis of new empowerment techniques appearing on the market.

5.3 Creation of a standard query for anti-counterfeiting technologies within the JRC's Technology Innovations Monitoring tool (TIM)

The JRC has created the Technology Innovation Monitoring tool (TIM), an instrument studied to allow users to monitor technologies in the market and their update and evolution. Precisely, the tool aims not only to describe and evaluate technologies, but also to provide a decision-making support methodology with a view also to market related issues. The tool might be used specifically to help users develop awareness and monitor technologies that can assist against counterfeiting better. The Observatory might have a role in this, through a standard query that might be created for it and its stakeholders, to monitor anti-counterfeiting technologies.

Suggestion 3): create a standard query in TIM specifically to enable the abovementioned expert group and the Observatory stakeholders to monitor the evolution of applicable anti-counterfeiting technologies.

5.4 Definition of an awareness programme to detect counterfeit goods through a smartphone

Awareness of the presence and features of counterfeit goods on the market through a smartphone is a simple but effective technique to fight the distribution of counterfeit products for various categories of consumers. Retailers and manufacturers can work together to provide awareness solutions, mobile applications and websites. To avoid fragmentation of the different solutions and to harmonise the search and presentation of the information required to identify a counterfeit product, standards and guidelines should be put in place and a central knowledge management repository should be set up. In Europe, the European Union Intellectual Property Office (EUIPO) could have a role to implement the central knowledge management repository through the Observatory.

Suggestion 4): implement an awareness knowledge management repository at European level in collaboration with retailers and manufacturers to be used and accessed through smartphones.

References

[1]. EC (2007). Consumer Policy Strategy 2007-2013, 'Empowering consumers, enhancing their welfare, effectively protecting them' (COM(2007) 99 final).

[2]. Wathieu, L., et al. (2002). Consumer Control and Empowerment: A Primer. Marketing. Letters, 13(3), 297-305.

[3]. Brennan, C., Ritters, K.(2004). Consumer Education in the UK: New Developments in Policy, Strategy, and Implementation. International Journal of Consumer Studies, 28 (March), 97-107.

[4]. Davison, M. (2011). Pharmaceutical anti-counterfeiting: combating the real danger from fake drugs. John Wiley & Sons.

[5]. Rust, R., Oliver, R. (1994). Video Dial Tone – The New World of Services Marketing. Journal of Services Marketing, 8 (3), 5-16.

[6]. Phuc (2015). Deputy PM Phuc urges promoting community empowerment in fighting against counterfeiting. http://en.nhandan.org.vn/society/legal/item/3430702-deputy-pm-phuc-urges-promoting-community-empowerment-in-fighting-against-counterfeiting.html. Last accessed 15 December 2015.

[7]. Miliard (2012). Rx anti-counterfeiting technologies to reach $1.2B by 2015. http://www.healthcareitnews.com/news/rx-anti-counterfeiting-technologies-reach-12b-2015. Last Accessed 15 December 2015.

[8]. WTMR (2014) Anti-counterfeiting apps on the rise, but consumer take-up remains a challenge. http://www.worldtrademarkreview.com/Blog/detail.aspx?g=31c7fd36-3aca-4fb9-aae6-ea75428e852e.

[9]. Bilcare 2015 Smart Devices by Adrian Burden at BilcareTechnologies http://www.bilcaretech.com/pdf/whitepaper/Technology-has-a-habit-of-converging.pdf. Last accessed August 2015.

[10]. PC World. NEC smartphone tech can spot counterfeit goods http://www.pcworld.idg.com.au/article/559250/nec-smartphone-tech-can-spot-counterfeit-goods/. 10 November 2014.

[11]. CODENTIFY 2015. http://www.dcta-global.com/our-mission.html. Last accessed 12 December 2015.

[12]. SICPATRACE (2015). http://www.sicpa.com/government-security-solutions/sicpatrace. Last accessed 2 December 2015.

[13]. AUTHENTICATEIT (2015). http://authenticateit.com/. Last accessed 2 December 2015.

[14]. uFaker (2015). https://www.ufaker.com/. Last accessed 2 December 2015.

[15]. GS1 http://www.gs1.org/docs/barcodes/GS1_General_Specifications.pdf. Last accessed 2 December 2015.

[16]. (ATT 2015) Seal Vector. http://www.att-fr.com. Last Accessed 12 December 2015.

[17]. VERIFYME (2015). http://www.verifyme.com/new-blog/2015/9/22/verifyme-receives-notice-of-allowance-for-authenticating-security-marks-on-material-goods-with-a-smartphone-app.

[18]. Arjo (2015). http://www.arjo-solutions.com/en/. Last accessed 2 December 2015.

[19]. ProofTag (2015). http://www.prooftag.net/solutions-2/authentication-technologies/. Last accessed 2 December 2015.

[20]. Rytter, W. (2000). Compressed and fully compressed pattern matching in one and two dimensions. Proceedings of the IEEE, 88(11), 1769-1778.

[21]. NIST (2014). RFID Technology in Forensic Evidence Management: An Assessment of Barriers, Benefits, and Costs. http://www.nist.gov/manuscript-publication-search.cfm?pub_id=916133.

[22]. Anne E. Wilcock, Kathryn A. Boys, (2014) Reduce product counterfeiting: An integrated approach, Business Horizons, Volume 57, Issue 2, March–April 2014, Pages 279-288, ISSN 0007-6813, http://dx.doi.org/10.1016/j.bushor.2013.12.001.

[23]. Telecom Digest (2014). Booming Fake Phone Market in Nigeria http://www.ittelecomdigest.com/news/security/item/55-booming-fake-phone-market-in-nigeria. Last accessed 12 December 2015.

[24]. NOKOMIS (2014) http://www.nokomisinc.com/. Last accessed 12 December 2015.

[25]. Cobb, W.E.; Laspe, E.D.; Baldwin, R.O.; Temple, Michael A.; Kim, Y.C.,(2012), Intrinsic Physical-Layer Authentication of Integrated Circuits *IEEE Transactions on Information Forensics and Security,* vol.7, no.1, pp.14,24, Feb. 2012.

[26]. Williams, M.D.; Temple, Michael A.; Reising, D.R., 'Augmenting Bit-Level Network Security Using Physical Layer RF-DNA Fingerprinting', *Global Telecommunications Conference (GLOBECOM 2010), 2010 IEEE* , vol., no., pp.1,6, 6-10 Dec. 2010.

[27]. Kalyanaraman, R., (2015). Counterfeit or Not? Use a Spectrometer to Find Out. Anti-counterfeiting for Pharmaceutical and Medical Devices. http://www.anticounterfeitingpharma.com. Last Accessed 15 December 2015.

[28]. Anna Luczak, PhD , Ravi Kalyanaraman, Ph.D. (2014). Portable and Benchtop Raman Technologies for Product Authentication and Counterfeit Detection http://www.americanpharmaceuticalreview.com/Featured-Articles/169505-Portable-and-Benchtop-Raman-Technologies-for-Product-Authentication-and-Counterfeit-Detection/. Last Accessed 16 December 2015.

[29]. Feng Lu (2013), Xinxin Weng, Yifeng Chai, Yongjian Yang, Yinjia Yu, Gengli Duan, A novel identification system for counterfeit drugs based on portable Raman spectroscopy, Chemometrics and Intelligent Laboratory Systems, Volume 127, 15 August 2013, Pages 63-69, ISSN 0169-7439, http://dx.doi.org/10.1016/j.chemolab.2013.06.001.

[30]. O'Neil, R. Jee, G. Lee, A. Charvill and A. Moffat, (2008) 'Use of a portable near infrared spectrometer for the authentication of tablets and the detection of counterfeit versions', J. Near Infrared Spectrosc. 16(3), 327–333 (2008).

[31]. Villasenor, J., & Tehranipoor, M., (2013). Chop shop electronics. Spectrum, IEEE, 50(10), 41-45.

[32]. AERI 2015. Counterfeit Electronic Component Detection. http://www.aeri.com/counterfeit-electronic-component-detection/. Last Accessed 3/07/2015.

[33]. DARPA technology uncovers counterfeit microchips, October 2014. http://www.networkworld.com/article/2690353/security0/darpa-technology-uncovers-counterfeit-microchips.html. Last Accessed 14/07/2015.

[34]. Müller, C., and Garriga, M., and Campoy-Quiles, M. (2012). Patterned optical anisotropy in woven conjugated polymer systems, Applied Physics Letters, 101, 171907 (2012), DOI:http://dx.doi.org/10.1063/1.4764518.

[35]. WHO 1999. Counterfeit Drugs. Guidelines for the development of measures to combat counterfeit drugs.

[36]. WCO (2105). IPM Connected http://www.wcoipm.org/ipm-connected. Last accessed 10 August 2015.

[37]. GMA 2014. Grocery Manufacturers Association. Brand Protection and Supply Chain Integrity: Methods for Counterfeit Detection, Prevention and Deterrence A Best Practices Guide http://www.gmaonline.org/filemanager/Collaborating_with_Retailers/GMA_Inmar_Brand_Protection.pdf. Last accessed 12 December 2015.

[38]. SecurPharma Status Report 2016. http://www.securpharm.de/fileadmin/pdf/statusbericht/status_report_2016.pdf. Last accessed September 2016.

[39]. Eurogroup Consulting and Sovereign Border Solutions for the European Commission. Analysis and Feasibility Assessment Regarding EU systems for Tracking and Tracing of Tobacco Products and for Security Features. March 2015. http://ec.europa.eu/health/tobacco/docs/2015_tpd_tracking_tracing_frep_en.pdf. Last accessed September 2016.

[40]. Sovanta named Winner of SAP and Google Glass Challenge for Enterprise http://sovanta.com/Presse/sovanta_SAPandGoogleGlassChallenge2015Winners_SAP_review.pdf. Last accessed 22/12/2016.

List of abbreviations and definitions

CCP	Customs Organization Global Container Control Programme (CCP)
COAs	Certificate Of Authenticity (COAs)
COAs	Privilege Management Infrastructure (COAs)
EDS	Electron Dispersive Spectroscopy
EPC	EPC (electronic product code).
FTIR	Fourier Transform Infrared Spectroscopy
GNSS	Global Navigation Satellite Systems
GUI	Graphical User Interface
EUIPO	European Union Intellectual Property Office
IC	Integrated Circuits
IoT	Internet of Things (IoT)
IP	Intellectual Property
IPR	Intellectual Property Rights
ISO	International Organization for Standardization
NFC	Near Field Communication
NIR	Near-infrared spectroscopy
PET	Privacy Enhancing Technology
PUF	Physical Unclonable Function
RFID	Radio Frequency Identifier
SAM	Scanning Acoustic Microscopy
SEM	Scanning Electron Microscopy
TGA	Thermogravimetric Analysis
UHF	Ultra High Frequency
UV	Ultra-Violet
WHO	World Health Organization

List of figures

List of tables

Europe Direct is a service to help you find answers to your questions about the European Union.

Free phone number (*): 00 800 6 7 8 9 10 11
(*) Certain mobile telephone operators do not allow access to 00 800 numbers or these calls may be billed.

A great deal of additional information on the European Union is available on the internet.
It can be accessed through the Europa server http://europa.eu

How to obtain EU publications

Our publications are available from the EU bookshop (http://bookshop.europa.eu),
where you can place an order with the sales agent of your choice.

The Publications Office has a worldwide network of sales agents.

You can obtain their contact details by sending a fax to (352) 29 29-42758.

KJ-NA-28400-EN-N

JRC Mission

As the science and knowledge service of the European Commission, the Joint Research Centre's mission is to support EU policies with independent evidence throughout the whole policy cycle.

EU Science Hub
ec.europa.eu/jrc

@EU_ScienceHub

EU Science Hub - Joint Research Centre

Joint Research Centre

EU Science Hub

Publications Office

doi:10.2760/135671

ISBN 978-92-79-64952-3